Manual de utilidades & Trucosinternet

Redacción, publicidad, administración y suscripciones
San Sotero, 8. 4ª planta. 28037 Madrid.
Tel: 913 137 900. Fax: 913 273 704
Redacción y publicidad en Barcelona
Avenida Pompeu Fabra, 10-bajos. 08024 Barcelona.
Tel: 932 846 100. Fax: 932 103 052

Editorial

Editor
Javier Pérez Cortijo jcortijo@bpe.es

Coordinación
Eva M Carrasco ecarrasco@bpe.es



Redactores y colaboradores
Albert Cabello
(Aplicaciones, Paso a paso, Apéndices)
Eduardo Sánchez
(Paso a paso)
Juan Carlos López
(Aplicaciones, Apéndices)
Daniel G. Ríos
(Paso a paso, Apéndices)
Javier Pastor
(Anonimato en la Red)
José Plana
(Anonimato en la Red, Paso a paso)
David Onieva
(Anonimato en la Red, Apéndices)
Raúl Rubio
(Apéndices)
José Manuel Soto
(Aplicaciones)

TrucosinternetCD

Coordinador
Jesús Fernández Torres jesusf@bpe.es

Producción/ Maquetación

Jefe de Arte / Portada
Javier Herrero jherrero@bpe.es

Maquetación Carmen Herrero

Director de producción
Agustín Palomino agustinp@bpe.es
Preimpresión Color 4
Imprenta Gráficas Ruan
Encuadernación Lanza, S.A.
Distribución DISPAÑA. Avda. General Perón, 27. 7ª. 28020 Madrid
Tel: 914 179 530. Fax: 914 795 539.

México: Importador exclusivo: Cade, S.A. de C.V. Lago Ladoca, 216. Colonia Anahuac. Delegación: Miguel Hidalgo. 11320 México D. F. Telf.: 5254 2999. Fax: 5545 6879. *Distribución Estados:* CITEM. *Distribución D.F.:* Unión de voceadores

Publicidad

Director de Publicidad
Miguel Onieva
Publicidad Madrid Guadalupe Martín, Marién Cuervo, Pedro Núñez
Publicidad Barcelona
Mª del Carmen Ríos



Representantes en el extranjero
Europa/Oriente Medio: Global Media Europe Ltd. 32-34 Broadwick Street. London W1A 2HG. Tel: 44 207 316 9101. Fax: 44 207 316 9774. www.globalreps.com. advertising@globalreps.com.
EE UU/Canadá: Global Media USA LLC. 565 Commercial Street. 4th floor. San Francisco, CA 94111-3031. USA. Tel: 415 249 1620. Fax: 415 249 1630. www.globalreps.com. sjones@globalreps.com.
Taiwan: Acteam. Tel: 886 2 711 4833.
Bélgica/Holanda/Luxemburgo: Insight Publicitas. Tel: 31 2153 12042.

MANUAL DE UTILIDADES & TRUCOS INTERNET está editado por



business publications españa

Consejero Delegado
Antonio González Rodríguez

Director de Publicaciones
Ángel F. González afgonzal@bpe.es

Director Financiero
Ricardo Anguita

Director Área PCs
Fernando Claver fercla@bpe.es

MANUAL DE UTILIDADES & TRUCOS INTERNET pertenece a la APP (Asociación de Prensa Profesional).

Depósito Legal M-26866-2000

La evolución de Internet

Una vez más apostamos por Internet y por la mejor forma de conocer todas sus posibilidades: la información puntual, precisa y práctica sobre los mejores trucos para estar al día en el mundo de la Web. Este que tenéis en vuestras manos es el nuevo ejemplar del Manual de Utilidades y Trucos Internet, el cuarto que publicamos con la misma idea original que motivó la edición del primero de ellos, comunicar con lectores ávidos de datos útiles que les permitan conocer de forma exhaustiva todos los recovecos de la Red.

De nuevo, transmitimos una visión positiva y optimista sobre la Web ya que, a pesar de que el mundo empresarial asociado a Internet está buscando sacar rentabilidad a sus inversiones haciendo de la Web un entorno con menos servicios gratuitos, el usuario todavía puede encontrar respuesta a sus necesidades en páginas y sitios hechos exclusivamente por y para los internautas.

Si lo que buscáis es conocer de forma práctica las nuevas versiones Internet Explorer 6, Outlook Express 6, Netscape 6.2, FrontPage 2002 o saber cómo funcionan las listas de correo y la mensajería instantánea o cómo optimizar la descarga de ficheros o, incluso, cómo mantener el anonimato durante la navegación por Internet, en este Manual encontraréis la respuesta a todas vuestras dudas.

Gracias a la información actual y a todos estos útiles trucos, reflejados, por ejemplo, en cada edición de este ya clásico Manual, el internauta español está alcanzando su madurez como usuario de Internet en su ordenador personal. Pero ahora debe enfrentarse a lo que le deparará el futuro más próximo, debe saber cuál es la evolución de Internet: la Web móvil.

La Red sin cables, la portabilidad de la red de redes a las plataformas móviles, la cultura del *always-on* («siempre conectado»), está más cerca que nunca debido a la más que próxima aparición de los teléfonos móviles GPRS y UMTS. Dentro de muy poquito tiempo Internet estará en el bolsillo de todos (no de unos pocos como hasta ahora) y sabremos que la Web y su evolución habrá tenido sentido para más cosas de lo que hoy creemos. Sigamos apostando por Internet y «lo único» que obtendremos será una sorpresa tecnológica tras otra.



Eva M Carrasco
Coordinadora



Nº4

Manual de utilidades

Trucosinternet

SUMARIO

Trucos CD



Aplicaciones

Todos los trucos para aprovechar al máximo todas las ventajas de las nuevas versiones de Internet Explorer y Netscape además de mantener el PC a salvo con McAfee.



Anonimato en la Red

En este apartado incluimos interesantes temas que ayudarán a cualquier usuario a conocer las claves para mantener su identidad oculta, no sólo en la navegación por Internet sino también a la hora de utilizar el correo electrónico.



Paso a paso

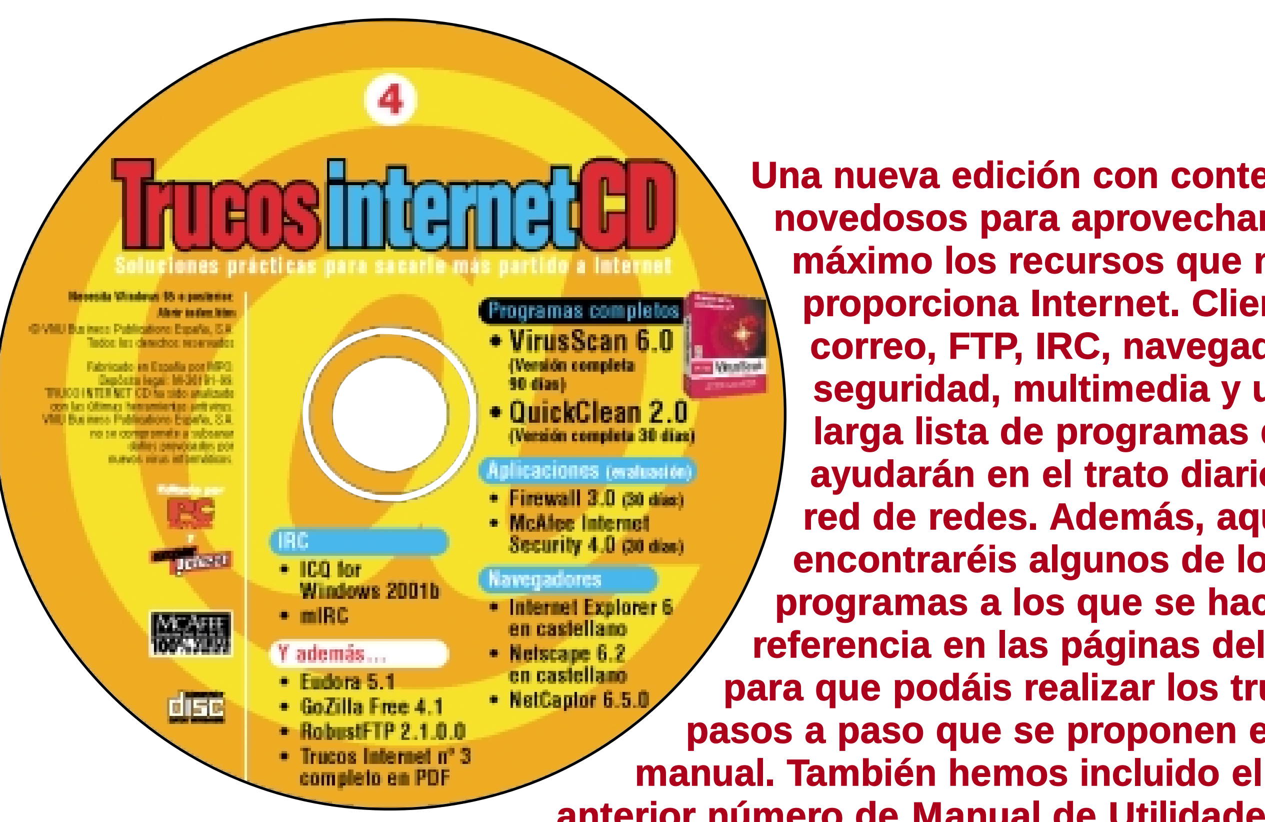
Explicamos hasta el más mínimo detalle todos los pasos necesarios para mejorar nuestra relación con la Red.



Apéndices y consejos útiles

Utilidades de navegación, correo electrónico, multimedia, seguridad...

El mejor compañero del internauta actual



Una nueva edición con contenidos novedosos para aprovechar al máximo los recursos que nos proporciona Internet. Clientes de correo, FTP, IRC, navegadores, seguridad, multimedia y una larga lista de programas que os ayudarán en el trato diario con la red de redes. Además, aquí encontraréis algunos de los programas a los que se hace referencia en las páginas del libro para que podáis realizar los trucos y pasos a paso que se proponen en el manual. También hemos incluido el anterior número de Manual de Utilidades y Trucos Internet en formato PDF.

Correo electrónico

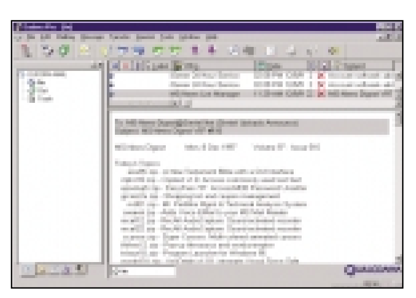
El uso del correo electrónico es algo tan cotidiano para cualquier persona, que no está de más actualizarse con otros clientes de correo o aprovechar las ventajas de nuevas utilidades para sacar el máximo partido a esta aplicación.

Eudora 5.1. Nueva versión del clásico cliente de correo electrónico. Sencillo y potente, permite mantener varias cuentas de correo.

SpamKiller 2.84. Elimina los mensajes que no queremos recibir, como los de publicidad.

AllegroMail 2.3.01. Permite administrar varias cuentas de correo e incluye una útil agenda de contactos.

JoMail 2.6.16. Sencillo cliente de correo que permite configurar varias cuentas y utilizar el correo a través de Web, como por ejemplo Hotmail.



Personaliza los mensajes de correo y gestiona nuestros contactos fácilmente.

IncrediMail 2001. Divertido cliente de correo que permite enviar mensajes personalizados con efectos 3D, sonido y animaciones.

Group Mail Free 3.4.03. Permite enviar mensajes a grupos de personas ordenados por categoría. Ideal para fines comerciales.

IRC

Las posibilidades de Internet son tan amplias que podemos aprovechar muchos de sus recursos con gran facilidad. En este apartado encontraréis programas de chat e IRC para que podáis comunicaros con vuestros amigos y/o grupos de charla.

ICQ for Windows 2001b. Atractivo programa de chat y localización instantánea de usuarios.

mIRC. uno de los clientes de IRC más utilizados. Soporta *scripts* y personalización de mensajes.



Chatead con vuestros amigos de una forma divertida y eficaz.

Mensajería instantánea

Otra de las opciones que ofrece la Red y que cada vez está teniendo más aceptación entre los internautas. Disfrutad de la mensajería instantánea con los programas que incluimos en este apartado.



Con una divertida interfaz, podréis comunicaros con vuestros amigos rápidamente.

AOLInstantMessenger. Programa de mensajería que permite intercambiar mensajes con usuarios de America Online.

MSN Messenger. Programa de mensajería instantánea de Microsoft muy amigable y sencillo de utilizar.

Odigo 3.1. Permite conectarnos con personas que visitan la misma página web, buscar personas por categorías y mucho más.

Trillian 0.6351. Permite utilizar diferentes cuentas y sistemas de programas como ICQ, Yahoo! o MSN, todo en el mismo programa.

Yahoo! Messenger 5.0. Es el sistema más rápido, efectivo y divertido para comunicarnos con los amigos a través de Internet.

Multimedia

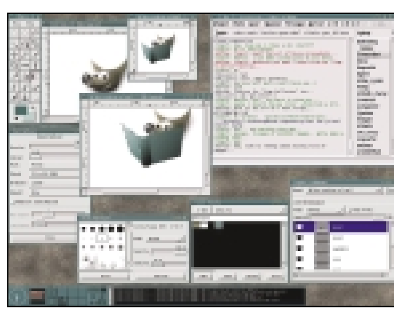
Esta sección se compone de varios programas multimedia, desde editores hasta reproductores de vídeo y audio.

ACDSee. Un excelente visor de ficheros gráficos. Soporta la mayoría de los formatos.

DirectX 8.1. Librerías de Microsoft para aprovechar el hardware de nuestro PC para aplicaciones multimedia y juegos.

DivX :-). Códec de vídeo DiVX para visualizar vídeo MPEG-4.

Gimp. Completo, potente y gratuito. Un rival freeware de Photoshop.



«Gimp» proporciona grandes posibilidades de edición gracias a sus herramientas.

ImageForge. Completo editor de imágenes con herramientas casi profesionales totalmente gratuito.

RealPlayer Basic. Visor de vídeo a través de Internet en formato Real.

Ulead PhotoImpact 7.0 Completo editor de imagen ideal para tus aplicaciones web.

Windows Media Player 7.1. Última versión del reproductor multimedia de Windows.

Programación

Editores de HTML, Javascript y utilidades varias para crear nuestras propias páginas web.

3D Webmaker 1.5. Programa para crear mundos virtuales para nuestra web.

CoffeeCupHTMLEditor. Rápido y sencillo editor de páginas HTML.

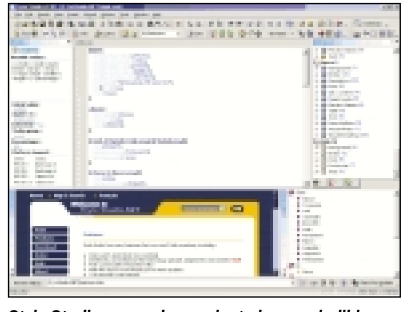
eMenuTree 2.0. Generador de menús para tu web.

HotDog. Completo editor de páginas web con herramientas visuales.

ScriptHackWizard. Editor de imágenes totalmente gratuito.

Stone's WebWriter 3.5. Editor HTML tanto para principiantes como para expertos.

Style Studio 2.02. Editor de hojas de estilo que te ayudará en la edición de tus webs.



Style Studio es una herramienta imprescindible para los diseñadores de páginas web.

TopStyle Lite 2.50. Otro editor y corrector de hojas de estilo.

WebScripter 3.1. Editor de código JavaScript con gran variedad de objetos para incluir en tus páginas.

Seguridad

Proteger nuestro ordenador de ataques de hackers, intrusos o simples curiosos puede ser una tarea ardua. Con estos programas, esperamos ayudaros.

Internet Access Scheduler. Permite activar o denegar el acceso a puertos de entrada/salida de TCP/UDP.

Anonimato en la Red. Varios programas necesarios para seguir el apartado dedicado a seguridad en las páginas del libro.

MindsoftSecurePack. Paquete de seguridad general para la conexión a Internet.

Kryptel Lite. Herramienta de encriptación con altos niveles de seguridad.

NetBrute Scanner Suite. Completo escáner de puertos para la detección de intrusos.

Supernaut. Programa de seguridad para la navegación por Internet.

Securo. Software de seguridad para la protección en las compras *on-line*.

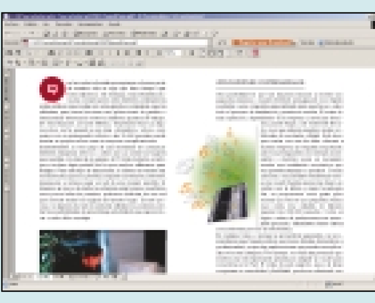
VisualRoute. Informa de las rutas de las conexiones.

TrojanDefense. Defiende nuestro PC de ataques de troyanos.

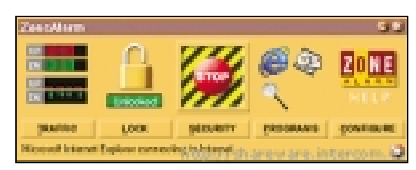
Manual de Utilidades & Trucos Internet 3



Para los que no pudieron disfrutar del anterior volumen de nuestro Manual o si queréis tener sus contenidos almacenados en vuestro disco duro, aquí tenéis el Manual de Utilidades & Trucos Internet 3 en formato PDF. Si queréis visualizar correctamente el libro debéis tener instalado el programa Adobe Acrobat Reader.



ZoneAlarm 2.6.362. Programa *proxy* para mantener la seguridad en nuestro PC.



Gestiona las comunicaciones de los programas que acceden a la Red.

McAfee

En este CD-ROM hemos incluido una sección especial que recoge varias herramientas de McAfee.

VirusScan 6.0. Es uno de los más potentes antivirus del mercado actual. Con esta versión de 90 días podréis mantener vuestro PC a salvo de cualquier «inquilino».

QuickClean 2.0. Limpia de forma exhaustiva el PC de ficheros innecesarios, aumentando el rendimiento y el espacio en disco.

Firewall 3.0. Una potente herramienta para la seguridad en Internet. Incluye Firewall 3 y VirusScan 6.

Internet Security 4.0. Mantiene vuestro PC fuera del alcance de intrusos y curiosos. Una forma sencilla de proteger nuestros datos de forma segura.

FTP

En esta sección incluimos varios clientes de FTP y gestores de descarga.

Download Accelerator Plus 5.0. Gestor de descargas que permite recuperar ficheros cortados.

Download Wiz 1.31. Permite descargar, mantener y gestionar los ficheros que bajamos de Internet.

FreeFTP 3.2. Cliente de FTP gratuito, sencillo de utilizar y con las funciones básicas de manipulación de ficheros.

GoZilla Free 4.1. Versión gratuita de este potente programa de descarga de ficheros.

NetAnts 1.25. Soporta múltiples conexiones a través de HTTP y FTP.

Simply COOL FTP! 1.0. Sencillo cliente de FTP que soporta múltiples conexiones y recuperación de ficheros cortados.

RobustFTP 2.1.0.0. Potente y seguro cliente de FTP que permite trabajar con ficheros de forma segura a través de la Red.

Esftp. Pequeño cliente de FTP con funciones básicas. Ideal para principiantes.

CuteFTP 4.2.5. Cliente de FTP con capacidades de búsqueda de archivos a través de la Red.

Miscelánea

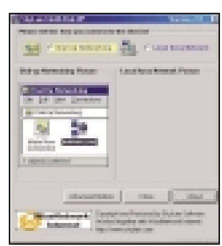
Una variedad de programas imprescindibles para vuestro PC. Desde compresores hasta aceleradores de conexión.

Alternativas Napster. Pequeña colección de utilidades para compartir ficheros de música entre usuarios personales.

Compresores. Varios de los compresores de ficheros más utilizados en Internet.

Free Agent 1.21. Lector de *News* gratuito que permite funcionar *off-line*.

Bookmark Manager 4. Gestor de direcciones y enlaces muy práctico y potente.



En esta versión completa podréis utilizar al máximo las opciones de aceleración de Intelli-Dial-UP.

Intelli-Dial-UP 2.51. Acelera la conexión a Internet modificando la configuración TCP/IP de tu PC.

FastNet99 4.1. Esta aplicación es idónea para acelerar nuestra conexión a Internet. Además incluye utilidades como Traceroute, Whois o Finger.

NetInfo 4.2. Proporciona extensa información sobre la conexión a Internet.

Genius 3.2.1. Recopilación de herramientas para Internet como Telnet, correo, FTP, Finger o Ping, entre otras.

Navegadores

Los mejores navegadores para que disfrutéis a tope de vuestra conexión a Internet.

Internet Explorer 6. Última versión del navegador de Microsoft. Incluye nuevas mejoras y resulta más rápido en la navegación por la web.

MSNExplorer 7. *Suite* de herramientas para navegar, gestionar tu correo Hotmail y muchas cosas más.

NetCaptor 6.5.0 Final. Navegador basado en Internet Explorer con multitarea.

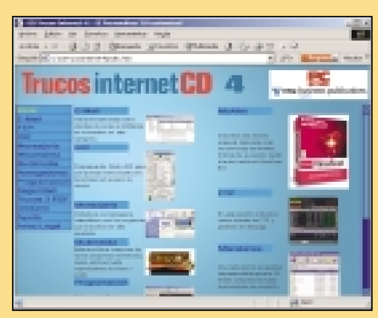
Netscape 6.2. Uno de los mejores navegadores con todo lo necesario para aprovechar Internet.

Opera 6.0 Bundled with JRE 1.3. Navegador multiventana con Java incorporado.

WinWAP 3.0. Navegador WAP para Windows.

Ejecución de TrucosCD

El CD-ROM se ejecuta automáticamente si tenéis la opción de autoarranque del sistema activada. En caso de que esté desactivado, sólo tenéis que ir al botón de *Inicio* de la *Barra de tareas* de Windows y seleccionar el comando *Ejecutar*. Entonces, en la línea de comandos indicaremos *D:\Index.htm*, donde D es la unidad del lector de CD-ROM.



El funcionamiento de la aplicación del CD es totalmente intuitivo. Como podréis observar, si hacéis clic en cualquiera de las opciones del menú principal, se desplegará otro menú que se encuentra dividido en secciones relativas a la misma. Podréis navegar entre las opciones hasta que lleguéis al último punto de la rama de menús donde se encuentran las aplicaciones que se incluyen en el CD. De esta forma, podréis encontrar de una forma rápida y sencilla la utilidad que buscáis. Una vez hayáis elegido la utilidad haciendo clic en el nombre, aparece en la parte inferior izquierda una descripción del mismo en el que se detalla el nombre, página web y sistema operativo entre otros. También veréis que, después de la descripción, aparece la ruta del programa dentro del compacto desde la cual podrás realizar la instalación haciendo clic en esta línea.
Si experimentáis problemas con la instalación o ejecución de alguno de los programas contenidos en el CD, comprobad que vuestro ordenador cumple los requisitos necesarios para realizar dichas operaciones. Si no podéis ejecutar algún programa desde el navegador del CD, intentad ejecutarlo directamente desde el directorio donde se encuentra.

CDs defectuosos

Si tu CD está deteriorado físicamente, envíalo a la dirección que se indica a continuación y te devolveremos otro en breve.

Departamento de suscripciones
C/ San Sotero, 8, 4ª planta
28037 MADRID



Internet Explorer 6.0

Ventajas y posibilidades del nuevo navegador

Internet Explorer 6 es probablemente la mejor versión del navegador de Microsoft liberada hasta la fecha. Forma parte de Windows XP en sus ediciones Home y Professional, donde se aplicarán los nuevos botones y estilos introducidos en la interfaz de usuario del SO dentro de la apariencia misma del navegador y los controles de páginas web; si bien puede también ser instalado en equipos con Windows 98, 98 Segunda edición, Millennium Edition, NT 4.0 y Windows 2000. Entre sus características destacan su fiabilidad y los intentos para mantener a salvo la privacidad de los usuarios, algo que se ha conseguido gracias a la implementación de las tecnologías de privacidad basadas en el nuevo estándar P3P (*Platform for Privacy Preferences*). Esas herramientas permiten controlar la información que las páginas web podrán recopilar sobre nosotros de una manera sencilla. Asimismo, las nuevas barras aumentan la flexibilidad del navegador, permitiéndonos simplificar tareas que realizamos diariamente, como son la búsqueda y reproducción de archivos multimedia, función que con la nueva *Barra multimedia* puede realizarse desde la ventana del explorador y sin necesidad de abrir aplicación alguna. El tratamiento de las imágenes también ha sido mejorado, incluyendo dos nuevas herramientas: el *cambio automático del tamaño* de las imágenes, que adaptará las dimensiones de las mismas al tamaño que tenga nuestra ventana del navegador, o la nueva *Barra de herramientas de imágenes*, que permitirá enviar por correo electrónico e imprimir de forma rápida y sencilla las imágenes que encuentre en páginas web. También con esta novedosa función hará posible ver todas las imágenes guardadas en la carpeta *Mis imágenes*, con tan sólo pasar el cursor por encima de una imagen contenida en una página HTML. Internet Explorer 6 es también la versión más estable y sin errores del navegador, y además incluye un nuevo servicio de recopilación de errores que ayudará a identificar los posibles problemas que puedan surgir para corregir en futuras actualizaciones del programa, todo ello cumpliendo con los estándares más estrictos en programación de páginas web y añadiendo soporte para nuevas tecnologías como XML y SOAP, de forma que se perfile como el cliente ideal de la futura plataforma. NET. En las próximas páginas encontraréis un buen número de trucos especialmente diseñados para Internet Explorer 6.0, si bien la mayoría de ellos también se podrán aplicar a versiones anteriores del cliente de Internet.



1 Requisitos mínimos de sistema

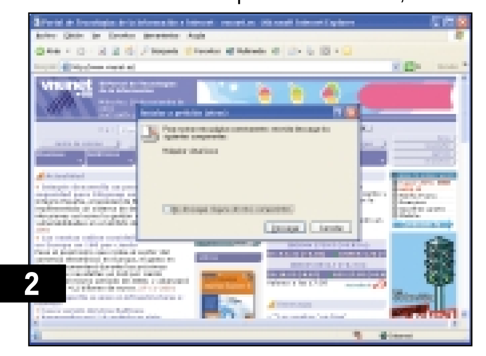
Básico

Procesador 486 a 66 MHz (se recomienda utilizar el procesador Pentium).
Microsoft Windows 98 y Windows 98 Segunda Edición:
16 Mytes de RAM como mínimo.
Tamaño de la instalación completa en Windows 98: 11,5 Mbytes.
Tamaño de la instalación completa en Windows 98 Segunda Edición: 12,4 Mbytes.
Windows NT® 4.0 Service Pack 6 y posterior:
32 Mbytes de RAM como mínimo.
Tamaño de la instalación completa: 12,7 Mbytes.
Windows 2000:
32 Mbytes de RAM como mínimo.
Tamaño de la instalación completa: 12 Mbytes.
Windows Millennium Edition:
32 Mbytes de RAM como mínimo.
Tamaño de la instalación completa: 8,7 Mbytes.

2 Soporte Java en Internet Explorer 6.0

Básico

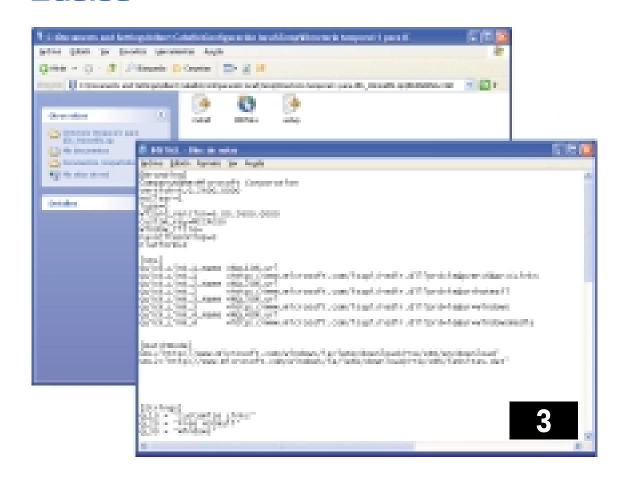
La distribución original de Internet Explorer 6.0 no incluye la máquina virtual Java, necesaria en muchos casos para el correcto funcionamiento de algunos componentes de las páginas web, si bien en aquellos equipos en que actualicemos nuestro navegador desde versiones anteriores, Internet Explorer adoptará el soporte de la máquina virtual Java ya existente. En los casos en que no dispongamos de la máquina virtual, como por ejemplo los usuarios de Windows XP, tendremos dos opciones para



conseguir nuestra máquina virtual Java: la primera, ir a la dirección *www.microsoft.com/java* y descargar la máquina virtual creada por Microsoft, o descargar la oficial de Sun desde la web *http://java.sun.com/getjava/installer.html*

3 Personalizar Internet Explorer

Básico



Si en anteriores números de este manual hemos explicado los pasos que teníamos que dar para eliminar las personalizaciones realizadas en una distribución de Internet Explorer modificada con el IEAK y distribuida por otro ensamblador, podemos realizar el camino inverso, es decir, personalizar nuestra propia instalación. En primer lugar, tendremos que extraer el archivo «install.ins» del archivo «branding.cab», para lo que necesitaremos tener instalada la herramienta Winzip o similar.

Este archivo «install.ins» es fácilmente editable con el bloc de notas («notepad.exe») y los parámetros que podemos modificar son los siguientes:

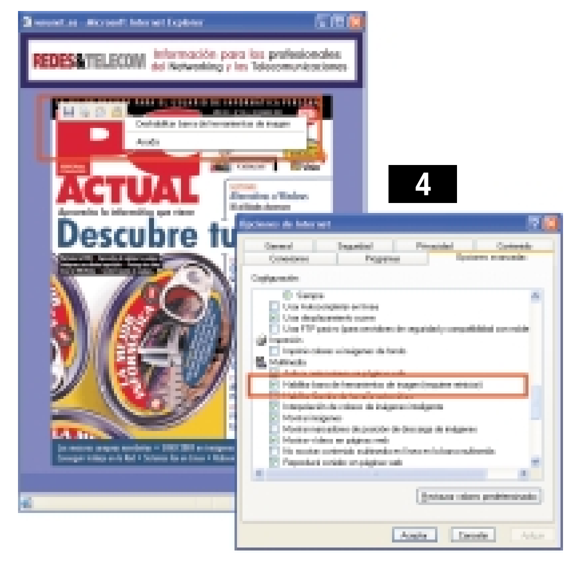
[Branding]
CompanyName=Manual de Trucos y Utilidades Internet
Window_Title=Internet Explorer proporcionado por Manual de Trucos y Utilidades Internet
[URL]
Quick_Link_1_Name =%QL10%.url
Quick_Link_1 =http://www.vnunet.es
Quick_Link_2_Name =%QL20%.url
Quick_Link_2 =http://www.pc-actual.com
Quick_Link_3_Name =%QL30%.url
Quick_Link_3 =http://www.computeridea.net
Quick_Link_4_Name =%QL40%.url
Quick_Link_4 =http://www.trucospc.com
[Strings]
QL10 = “Página corporativa de VNU España”
QL20 = “Página principal de la revista PC ACTUAL”
QL30 = “Página principal de la revista Computer Idea”
QL40 = “Página principal de la revista Trucos PC”

General y navegación

4 Desactivar la *Barra de herramientas de imágenes*

Intermedio

La *Barra de herramientas de imágenes* es una nueva funcionalidad añadida en Internet Explorer 6.0, que se muestra al situar el cursor encima de una imagen y nos permite guardar, imprimir,



enviar por correo o ver el contenido de la carpeta «Mis imágenes» de una forma rápida y sencilla. Sin embargo, si empieza a molestarnos el hecho de que ralentice en exceso nuestra navegación, podemos desactivarla de dos formas: la primera, a través del menú *Herramientas/Opciones de Internet*, desmarcando en la pestaña *Avanzada* la opción *Habilitar barra de herramientas de imagen*, o al situar el cursor sobre una imagen en una página web, haciendo clic con el botón derecho del ratón sobre la *Barra de herramientas de imágenes* y seleccionando la opción *Deshabilitar barra de herramientas de imágenes*.

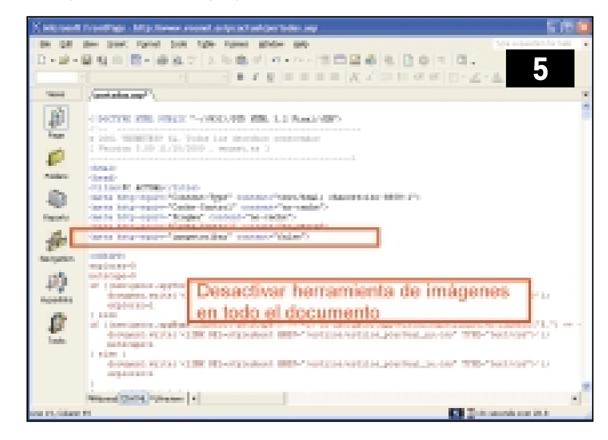
5 Desactivar la *Barra de herramientas de imágenes* en las páginas HTML

Intermedio

Como desarrolladores de contenidos, podremos deshabilitar o activar las funciones de la *Barra de herramientas de imágenes* para una imagen concreta o todas las imágenes en una página web. La sintaxis que hemos de introducir para desactivar las funciones en imágenes individuales deberá seguir la siguiente forma dentro del campo <img> en el código HTML de la página web:

<img border=“0” src=“filename” galleryimg=“no”> o <img border=“0” src=“filename” galleryimg=“false”>

Si queremos desactivar las funciones de la *Barra de herramientas de imágenes* para todas las imágenes en una página web, añadiremos la siguiente sintaxis en el campo <meta> del código HTML de la página web:

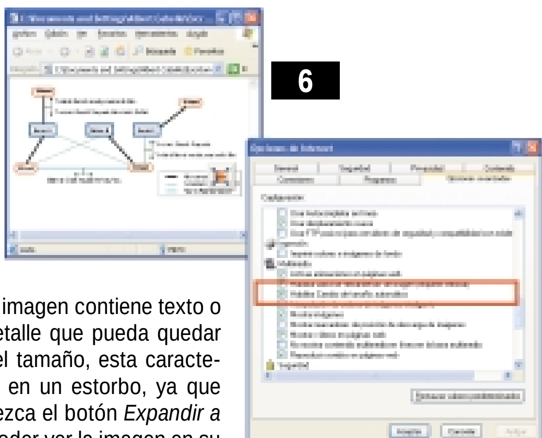


<meta http-equiv=“imagetoolbar” content=“no”> o <meta http-equiv=“imagetoolbar” content=“false”>
Si deshabilitamos las funciones de la *Barra de herramientas de imágenes* para todas las imágenes en una página web, también podremos activarla para alguna imagen en concreto, estableciendo el atributo *galleryimg* a “yes” o “true” dentro de la sintaxis del campo <img> en el código HTML de la página web:
<img border=“0” src=“filename” galleryimg=“yes”> o <img border=“0” src=“filename” galleryimg=“true”>

6 Cómo deshabilitar el cambio automático del tamaño de la imagen

Básico

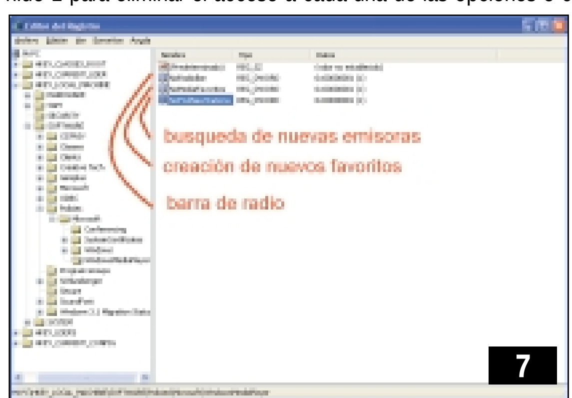
Por defecto, Internet Explorer adaptará automáticamente el tamaño de las imágenes que por su tamaño no quepan dentro de las dimensiones de la ventana del navegador, una función útil cuando tenemos que echar un vistazo rápido a una imagen o fotografía. Sin embargo, si la imagen contiene texto o cualquier otro tipo de detalle que pueda quedar distorsionado al alterar el tamaño, esta característica podrá convertirse en un estorbo, ya que será necesario que aparezca el botón *Expandir a su tamaño natural* para poder ver la imagen en su tamaño original. Para desactivarla, dentro del menú *Herramientas/Opciones de Internet* seleccionaremos la pestaña *Avanzada*. Bajo el apartado *Multimedia* desmarcaremos la casilla *Habilitar cambio de tamaño automático*.



7 Eliminar elementos del reproductor multimedia

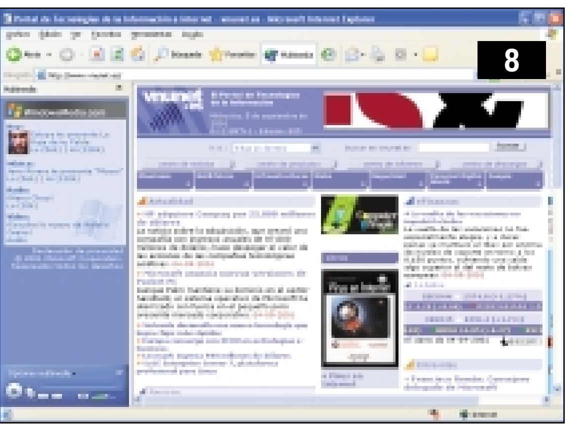
Intermedio

Este truco nos permitirá eliminar la *Barra de radio*, los *Favoritos* y la opción para buscar nuevas emisoras de radio en el reproductor de Windows Media. Iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejectuar* y localizaremos la clave *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsMediaPlayer*. Allí añadiremos un nuevo valor DWORD o modificaremos con el contenido 1 para eliminar el acceso a cada una de las opciones o 0 para continuar mostrándolas:
NoRadioBar (barra de radio)
NoMediaFavorites (creación de nuevos favoritos)
NoFindNewStations (búsqueda de nuevas emisoras)



8 Barra de medios

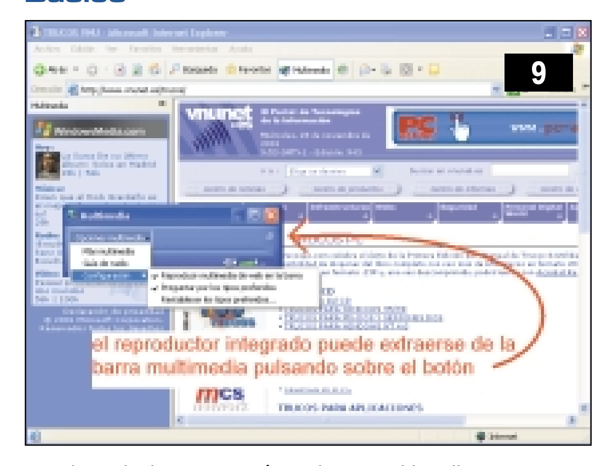
Básico



Si pulsamos sobre el botón *Multimedia* de la *Barra de herramientas* de Internet Explorer, aparecerá la nueva *Barra de medios*. Desde esta barra tendremos acceso directo a los contenidos del portal windowsmedia.com y a todas las emisoras de radio por Internet gracias al pequeño reproductor multimedia integrado que incluye, que nos permitirá reproducir los archivos desde la Web sin necesidad de abrir aplicaciones externas o una nueva ventana del navegador. Esta barra tiene controles simples que permiten reproducir vídeo, archivos mixtos y animaciones, pudiendo controlar el volumen y escoger los archivos de medios o pistas a reproducir.

9 Configurar las preferencias

Básico



Esta barra incluye un menú *Opciones multimedia* que nos permitirá localizar rápidamente archivos multimedia y establecer también las preferencias de funcionamiento.
Pulsando sobre el botón *Más multimedia* cargaremos en el área de navegación de Internet Explorer la página *www.windowsmedia.com* y en la *Barra de medios* las pestañas *Música, Películas, Radio y Entretenimiento,* que utilizaremos para localizar los archivos multimedia que queramos reproducir.
En la *Guía de radio* de windowsmedia.com, seleccionaremos una de la lista de estaciones predefinidas o utilizaremos el buscador de emisoras para localizar la emisora que queremos escuchar.

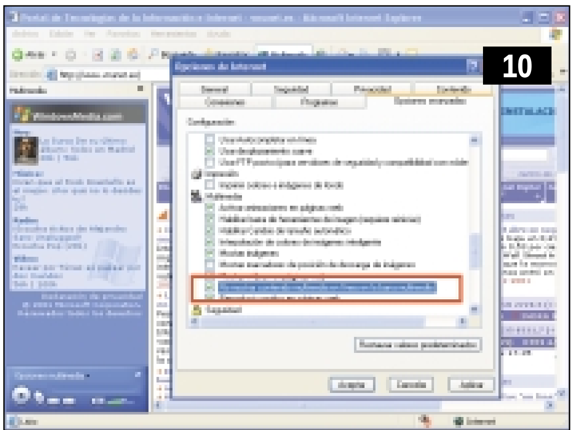
Si queremos establecer las preferencias de la *Barra de medios*, pulsaremos sobre la opción *Configuración* y marcaremos o desmarcaremos cualquiera de las siguientes opciones:

-*Reproducir multimedia de web en barra*: sirve para reproducir automáticamente los archivos multimedia existentes en páginas web dentro de la *Barra de medios* en vez de en el reproductor multimedia predeterminado, opción activada por defecto.

-*Preguntar por los tipos preferidos*: esta opción hace que, al abrir un archivo de medios desde una página web, aparezca un cuadro de diálogo que nos pregunte si queremos reproducir el archivo en la *Barra de medios* o desde el reproductor de Windows Media. Si escogemos esta opción, en el futuro todos los archivos con el mismo formato serán abiertos en la *Barra de medios*.

10 Desactivar el contenido multimedia *on-line* en la *Barra de medios*

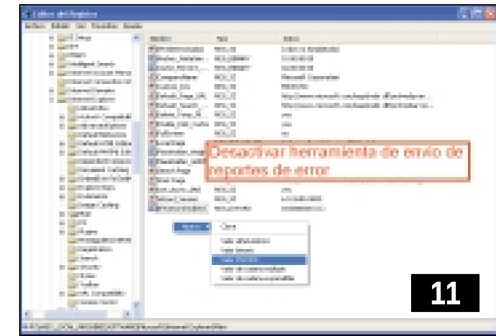
Intermedio



Si nuestro ordenador está conectado a Internet, cuando activemos la *Barra de medios* automáticamente contactaremos con el servidor windowsmedia.com y se descargarán contenidos multimedia en línea. Podemos desactivar la descarga y visualización de contenido multimedia en línea a través de la *Barra de medios* para que no muestre estos contenidos desde el menú *Herramientas/Opciones de Internet* bajo la pestaña *Opciones Avanzadas*. Para ello, activaremos la marca de la casilla *No mostrar contenido multimedia en línea en la barra multimedia*.

11 Controlar la herramienta de informe de errores

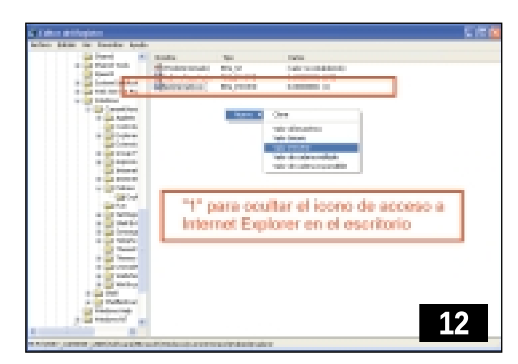
Intermedio



Esta herramienta se encuentra activada por defecto y se encarga de remitir de forma anónima a Microsoft los errores que se produzcan dentro del navegador para corregir su funcionamiento. Mediante la edición del registro podemos controlar el comportamiento de esta herramienta y desactivar su uso. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar*. Localizaremos la clave *HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main* y crearemos o modificaremos el valor DWORD existente (IEWatsonDisabled) cuyo contenido será 1 para desactivar la herramienta o 0 para activar el envío de errores.

12 Ocultar el icono *Internet Explorer* del *Escritorio*

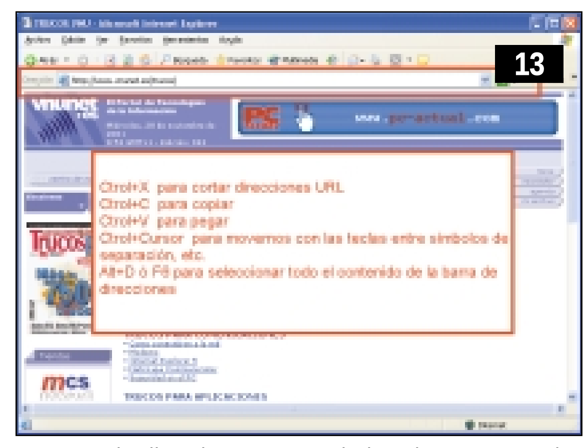
Intermedio



Si utilizamos otro programa diferente de Internet Explorer como navegador predeterminado, el icono *Internet Explorer* mostrado en el *Escritorio* será un problema para nosotros. Si bien en equipos con Windows XP resulta fácil ocultar este icono (a través de las *Propiedades de pantalla*, bajo la pestaña *Escritorio*, pulsando sobre el botón *Personalizar escritorio*), en Sistemas Operativos anteriores tendremos que pelearnos con el registro para ocultarlo. Iniciaremos el editor del registro de Windows con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*. Allí crearemos o modificaremos el valor DWORD existente (NoInternetIcon) cuyo contenido será 1 para ocultar el icono o 0 para continuar mostrándolo.

13 Atajos de teclado para la *Barra de direcciones*

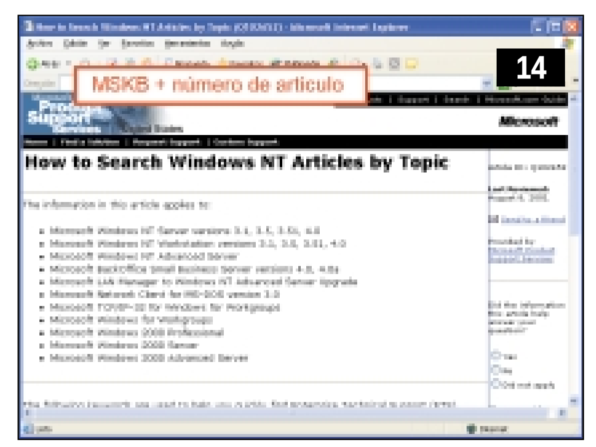
Básico



La *Barra de direcciones* es uno de los elementos con los que más nos pelearemos a la hora de trabajar con Internet Explorer. Para facilitar nuestro trabajo, podemos utilizar los atajos de teclado clásicos del bloc de notas («Ctrl+X» para cortar direcciones URL, «Ctrl+C» para copiar, «Ctrol+V» para pegar, movernos con las teclas «Ctrl+Cursor» entre símbolos de separación, etc.) Además podemos seleccionar todo el contenido de la *Barra de direcciones* con la combinación de teclas «Alt+D» o «F6», y también tendremos la posibilidad de hacer clic una sola vez sobre ella para ver todo su contenido.

14 Recuperar un articulo de la *Knowledge base*

Intermedio

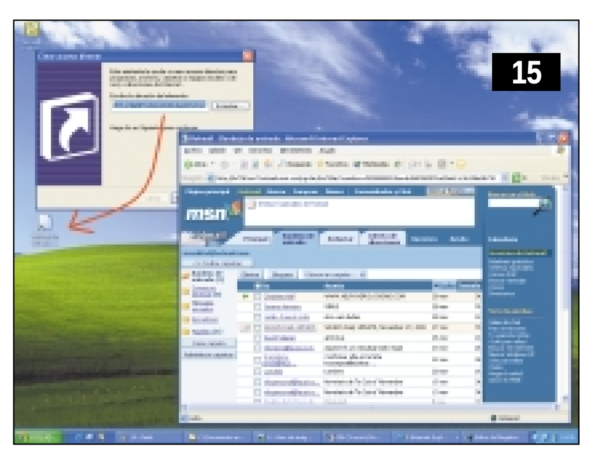


Los archivos de la *Knowledge base* de Microsoft utilizan una convención numérica que fácilmente podemos trasladar a la dirección URL del artículo, de forma que por ejemplo, para recuperar el archivo Q102652, escribiríamos la dirección URL *http://support.microsoft.com/support/kb/articles/Q102/6/52.asp*. Sin embargo, si conocemos la identificación de un artículo de la *Knowledge base* de Microsoft, podemos utilizar un método mucho más rápido para recuperar de manera automática el archivo, consistente en introducir en la *Barra de direcciones* de nuestro navegador el comando «mskb 102652». Automáticamente la herramienta de búsqueda del navegador enlazará con la página *http://support.microsoft.com/support/misc/kblookup.asp?id102652* para recuperar el artículo. Sin embargo, Internet Explorer deberá tener establecido como idioma principal dentro del menú *Herramientas/Opciones de internet/General/Lenguaje* el inglés, con lo que los contenidos de muchas páginas quedarán personalizados en este idioma.

15 Acceso directo a cuentas de Hotmail

Básico

Este truco puede ser utilizado para crear un acceso directo que enlazará automáticamente la *Bandeja de entrada* de nuestra cuenta de correo electrónico en el servicio gratuito Hotmail. Haremos clic con el botón derecho del ratón sobre un área vacía del escritorio y seleccionaremos el menú *Nuevo/Acceso directo*, estableciendo en la casilla *Escriba la ubicación del*



elemento el siguiente comando dependiendo del sistema operativo que tengamos:

Windows NT/2000/XP:

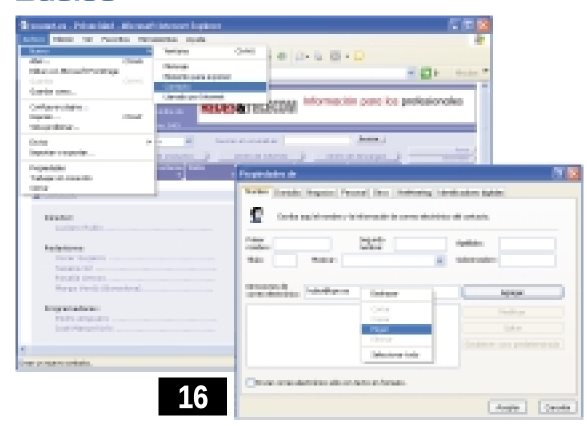
%WINDIR%\SYSTEM32\rundll32.exe "%PROGRAMFILES%\INTERNET EXPLORER\hmmapi.dll",OpenInboxHandler

Equipos Windows 9x/Me:

rundll32 "C:\ARCHIVOS DE PROGRAMA\INTERNET EXPLORER\hmmapi.dll",OpenInboxHandler

16 Añadir automáticamente direcciones *e-mail* a la *Libreta de contactos*

Básico



Si utilizamos Internet Explorer como navegador predeterminado, estaremos permanentemente conectados a nuestras aplicaciones para la gestión de contactos, correo, agenda, foros de noticias y llamadas de Internet. Prueba de ello es que desde el menú *Archivo* del navegador, seleccionando la opción *Nuevo/Contacto,* podremos abrir la *Libreta de contactos* y a través de ella introducir la información de contacto copiando y pegando el texto directamente desde un enlace en una página web a la libreta de direcciones. Adicionalmente, si pulsamos en nuestro navegador el enlace a una dirección de correo electrónico, automáticamente abriremos nuestro gestor de correo con la cuenta configurada como predeterminada para enviar un nuevo mensaje.

17 Abrir nuevas ventanas en modo maximizado

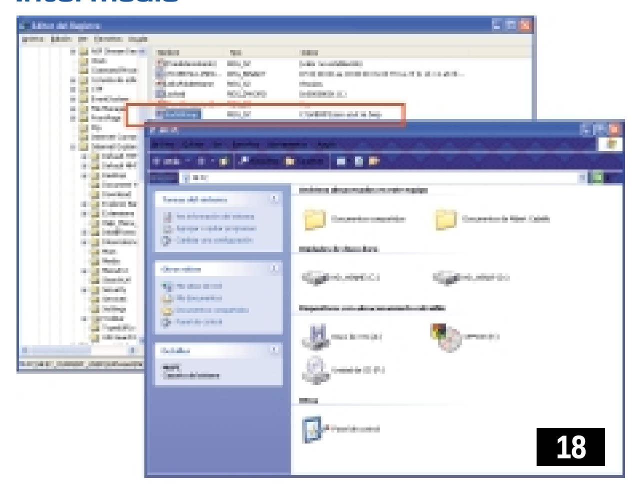
Intermedio

Cuando estemos trabajando con Internet Explorer, en ocasiones necesitaremos utilizar todo el espacio que nuestro monitor nos permita. Para ello, maximizaremos el contenido de las ventanas a través del botón existente en la parte superior derecha de la aplicación. Si pulsamos sobre el botón *Maximizar* en la ventana de Internet Explorer y más tarde sobre el botón *Cerrar*, simbolizado por un aspa roja, Internet Explorer se abrirá en modo maximizado la próxima vez que iniciemos la aplicación. Este comportamiento también lo podemos trasladar a las nuevas ventanas que abrimos al seleccionar un enlace con el menú contextual *Abrir nuevas ventanas* del navegador. Desde Internet Explorer abriremos el enlace de una página web en una nueva ventana, a través del menú contextual. Acto seguido, nos situaremos sobre la primera ventana que abrimos y la cerraremos (este paso es muy importante). Volveremos a la nueva ventana abierta recientemente y le modificaremos el

tamaño a nuestro antojo, pero sin utilizar el botón *Maximizar*. Cerraremos la ventana del navegador. De esta forma, en adelante cuando abramos una nueva ventana del navegador, se abrirá en este nuevo tamaño personalizado que acabamos de configurar.

18 *Background/Toolbar Wallpaper*

Intermedio

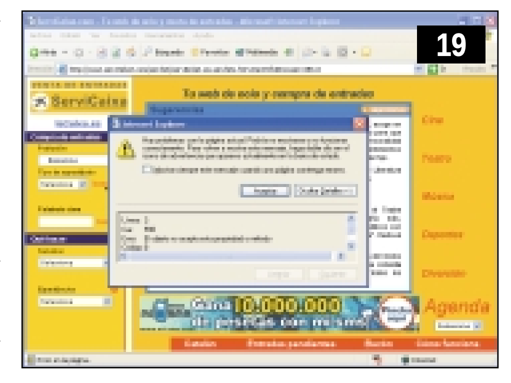

18

Si utilizamos la herramienta *Toolbar Wallpaper* desde el sitio de Microsoft en *www.microsoft.com/Windows/ie/previous/webaccess/tbwlpapr.asp*, cambiar la imagen de fondo que aparece en la *Barra de herramientas* del navegador se convertirá en un juego de niños. Si queremos añadir una imagen a la *Barra de herramientas* del *Explorador de Windows*, siempre que seamos usuarios de versiones superiores a IE 4.0, podremos hacerlo iniciando la herramienta de edición del registro del sistema utilizando el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizando la clave *HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar*. Allí crearemos un nuevo valor alfanumérico con el nombre BackBitmap, y cuyo contenido será la ruta de nuestro archivo de mapa de bits favorito. Los cambios surtirán efecto de forma automática. Para eliminar la imagen, eliminaremos el contenido de la clave creada.

19 Controlar el depurador de *scripts* de Internet Explorer

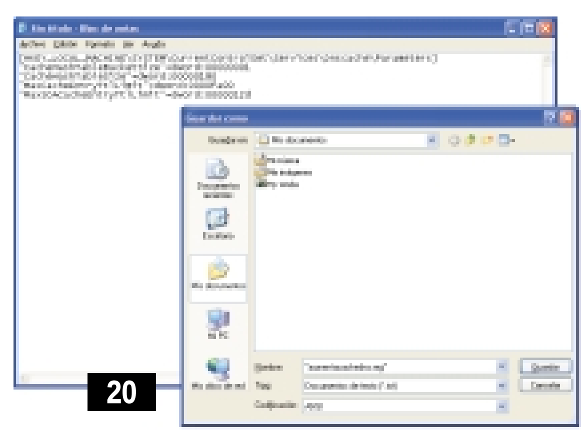
Intermedio

Cuando Internet Explorer detecta un error al procesar las instrucciones incluidas en un *script* de una página web, tenemos la posibilidad de lanzar un depurador que nos ayudará a diagnosticar el problema. La configuración de este depurador se encuentra, dentro del menú *Herramientas/Opciones de Internet* bajo la pestaña *Opciones Avanzadas*, en el apartado *Examinar* con el nombre *Desactivar depurador de secuencias de comandos,* cuya casilla marcaremos o desmarcaremos dependiendo si queremos utilizar esta funcionalidad, que en algunos equipos ralentiza sensiblemente la navegación.


19

20 Acelerar la navegación en sistemas Windows XP

Avanzado


20

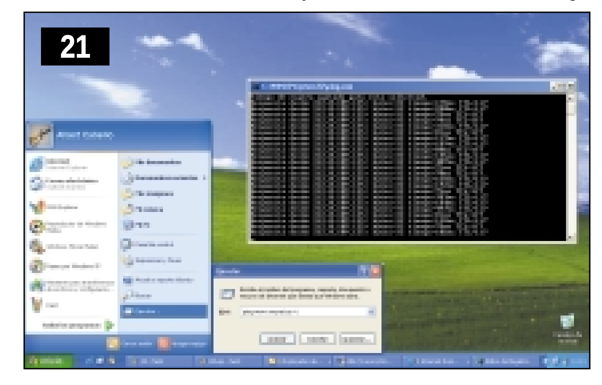
Cuando nos conectamos a un sitio web, la conexión entre nuestro navegador y el servidor remoto funciona de forma bidireccional: enviando y recibiendo información, esto es obvio. Parte de esta información se refiere a la resolución del nombre del sitio web en una dirección IP, trabajo del que realmente se encarga el protocolo TCP/IP. Esta información DNS queda registrada de forma que nuestro equipo no necesitará preguntar la localización del sitio cada vez que visitemos la página. Aunque Windows XP y Windows 2000 tienen una caché DNS bastante eficiente, podemos incrementar su rendimiento aumentando su tamaño. Para ello copiaremos el siguiente texto dentro del bloc de notas «notepad.exe», salvaremos el archivo como «aumentacachedns.reg» e introduciremos su contenido en el registro haciendo doble clic sobre el mismo.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters]
“CacheHashTableBucketSize”=dword:00000001
“CacheHashTableSize”=dword:00000180
“MaxCacheEntryTtlLimit”=dword:0000fa00
“MaxSOACacheEntryTtlLimit”=dword:0000012d
```

21 Mantener la conexión activa

Intermedio

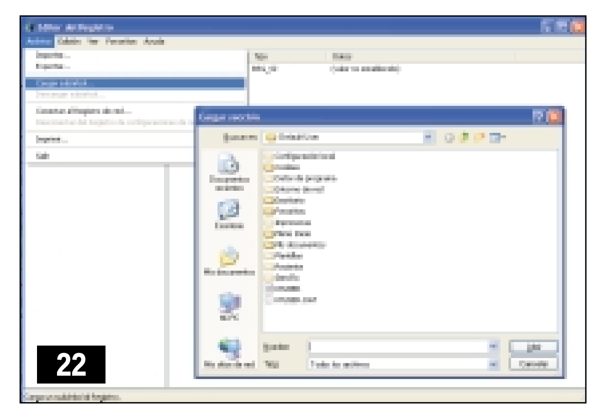
Dejar nuestras aplicaciones de Internet solas por más de unos minutos puede significar perder nuestra conexión y, por tanto, el trabajo que estemos realizando o los archivos que estemos descargando. Existen varios métodos para mantenerla funcionando, incluso en periodos de inactividad. Uno de ellos es abriendo nuestro menú *Inicio* y dentro del cuadro de diálogo


21

Ejecutar escribir el comando «PING www.servidor.com –t». Tras esto minimizaremos la ventana para que funcione en segundo plano. El parámetro -t utilizado tendrá como consecuencia que el *ping* sobre el servidor especificado será continuo, manteniendo de esta forma nuestra conexión activa. Cuando estemos listos para continuar nuestro trabajo, volveremos a la ventana del intérprete de comandos y pulsaremos la combinación de teclas «Ctrl+C» para detenerlo.

22 Evitar el funcionamiento del *Asistente para Conexión a Internet*

Intermedio

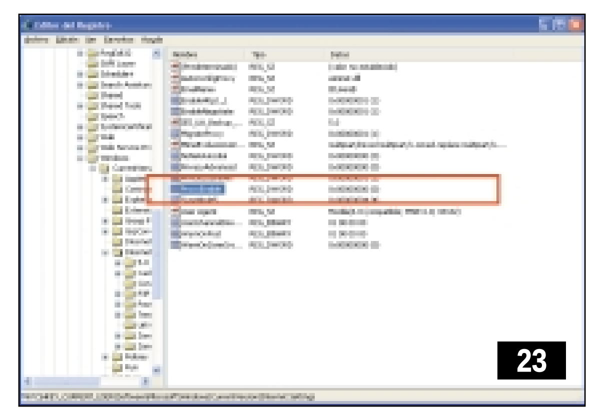


En equipos NT-2000-XP, cada vez que un nuevo usuario se conecta a Internet por primera vez, el asistente para conexión a Internet será lanzado automáticamente. Sin embargo, podemos modificar el perfil predeterminado para los nuevos usuarios de forma que no se invoque al programa. Para ello iniciaremos la herramienta de edición del registro del sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar*, y haremos clic sobre la clave *HKEY_LOCAL_MACHINE*. Una vez hecho esto, dentro del menú *Archivo/cargar subarbol* abriremos el archivo del perfil de nuevos usuarios, que se encuentra en *\Documents and Settings\Default User\ntUSER.DAT* y llamaremos la nueva clave "AAAA". Navegaremos hasta la clave *HKEY_LOCAL_MACHINE\AAAA\Software\Microsoft\Internet Connection Wizard*. Allí crearemos un nuevo valor DWORD o modificaremos el existente «Completed» cuyo contenido será 0 o 1 dependiendo si queremos mostrar en los nuevos perfiles el *Asistente para Conexión a Internet* o no. Una vez hecho esto, seleccionaremos la clave *HKEY_LOCAL_MACHINE\AAAA* y descargaremos la rama mediante el menú *Archivo/descargar subarbol*.

23 Configuración del servidor *proxy*

Intermedio

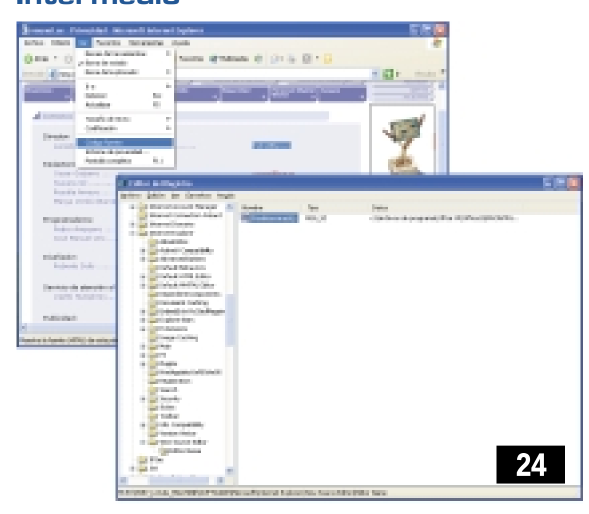
Si necesitamos configurar el mismo servidor *proxy* para Internet Explorer en múltiples ordenadores, o simplemente queremos automatizar el procedimiento a través de las posibilidades que nos ofrece el sistema, esta es la manera. Iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings*. Los valores que configuran el *proxy* de Internet se encuentran en esta clave. Para cambiar el servidor *proxy* utilizado, modificaremos el valor de la clave ProxyServer que equivaldrá al servidor y la combinación de puertos. Por ejemplo, si nuestro servidor *proxy* se llama \PROXY y está funcionando en el puerto 80,



estableceremos el ajuste como PROXY:80. También necesitaremos establecer el valor de la clave ProxyEnable a 1 para activar el *proxy* o 0 para desactivarlo. Introduciendo en la clave ProxyOverride el contenido <local> evitaremos que las direcciones internas pasen a través del *proxy*. Los cambios surten efecto inmediatamente.

24 Usar un programa alternativo para ver el código fuente

Intermedio



Por defecto, cuando usamos la función *Ver código fuente* de Internet Explorer, el programa asociado a esta función que se iniciará será el bloc de notas de Windows. Con este truco podremos escoger el editor que se utilizará. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\View Source Editor\Editor Name*. Allí modificaremos el contenido del valor alfanumérico (Predeterminado) con la ruta completa y nombre del archivo del editor que utilizaremos para ver el contenido HTML de las páginas web. Reiniciaremos Internet Explorer para que los cambios surtan efecto.

25 Modificar las páginas de error

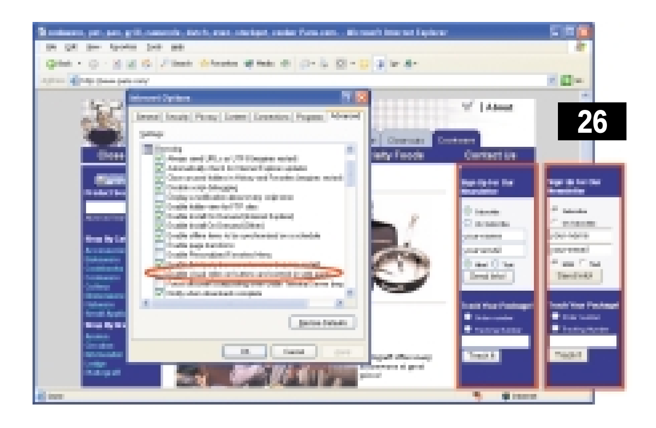
Intermedio

Las páginas de error que Internet Explorer muestra cuando se dan circunstancias como la navegación cancelada, navegación fallida, información fuera de línea y página en blanco se encuentran incluidas dentro de los archivos «mshtml.dll» y «shdoclc.dll»

en las subcarpetas de instalación del sistema, y su uso se halla configurado dentro del registro de Windows. Podemos reemplazar la visualización de estas páginas con las nuestras propias si queremos personalizar la navegación de Internet Explorer cuando ocurra alguno de estos eventos. Para ello iniciaremos la herramienta de edición del registro del sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar y localizaremos la clave* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs. Allí modificaremos el contenido de los valores alfanuméricos blank, DesktopItemNavigationFailure, mozilla, NavigationCancelled, NavigationFailure, OfflineInformation y PostNotCached con la ruta completa de la nueva página que se mostrará ante los diferentes sucesos de error. Estas páginas podremos cargarlas en nuestro navegador introduciendo el comando *:about valor*, como por ejemplo about:NavigationFailure.

26 Integración con temas visuales

Básico

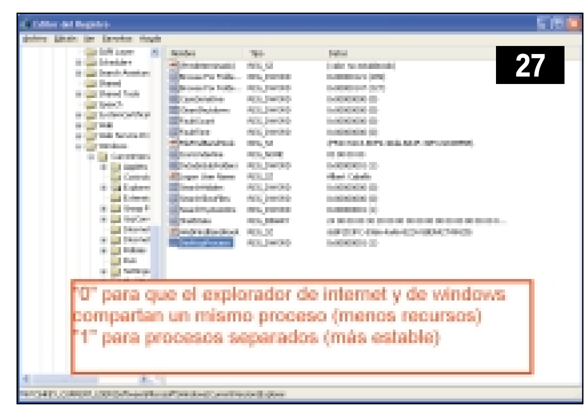


Fruto de la integración entre Windows XP e Internet Explorer 6.0 se da una característica que permite adaptar los controles de las páginas (botones, cajas, marcadores…) según la apariencia del tema de escritorio de Windows XP que estemos utilizando. Esta opción la encontraremos dentro del menú *Herramientas/Opciones de Internet* bajo la pestaña *Avanzada,* marcando la casilla *Permitir estilos visuales en botones y controles de las páginas web*.

27 Crear procesos separados para el *Escritorio* e Internet Explorer

Avanzado

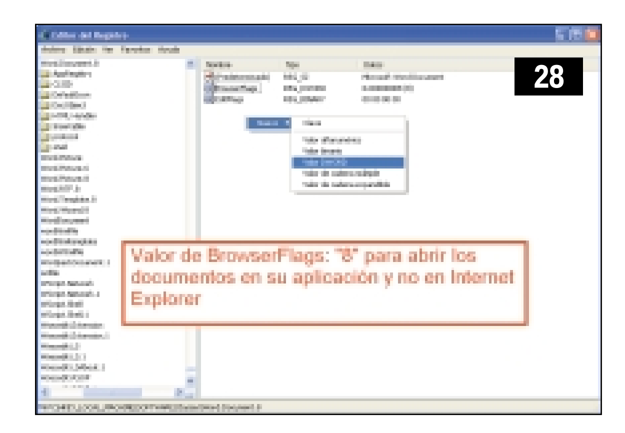
Por defecto, Windows crea un único proceso «explorer.exe» dividido en varios hilos encargados de la gestión y funcionamiento del *Escritorio*, la *Barra de tareas* y todas las otras instancias del *Explorador* de Windows y el navegador Internet Explorer. Debido a la íntima relación entre navegador y SO, si una de estas instancias falla, todas las demás fallarán. Modificando este comportamiento, Windows creará procesos separados



previniendo y aislando los fallos que puedan producirse, aun a cargo de un mayor consumo de recursos del sistema. Para ello iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer*. Allí crearemos o modificaremos el valor DWORD DesktopProcess, cuyo contenido estableceremos con 1 para crear procesos separados o 0 para utilizar el mismo proceso (opción predeterminada). Deberemos reiniciar Windows para que los cambios surtan efecto.

28 Documentos de Office que se abren en Internet Explorer

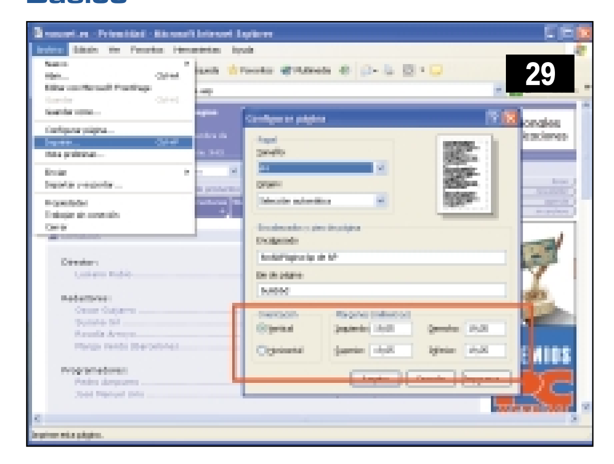
Básico



En algunos sistemas, cuando hagamos clic en un enlace a un archivo de Office, este archivo podrá abrirse, como si de un *plug-in* se tratara, dentro de la misma ventana de Internet Explorer, en vez de en la aplicación de Office correspondiente. Este es un comportamiento que se puede configurar mediante la edición del registro. Para ello, iniciaremos la herramienta con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la extensión del documento de Office que queramos modificar, bajo la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Classes*. Usaremos la cadena del valor (Predeterminado) para navegar hacia la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Valor de (Predeterminado)*. Por ejemplo, si estamos usando Excel 2002, el valor de la cadena (Predeterminado) de la extensión «.xls» contiene Excel.Sheet.8, de forma que tendremos que navegar hacia *HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.8*. Una vez seleccionada esa subclave, añadiremos un valor DWORD BrowserFlags, cuyo contenido será 8. Este proceso podremos repetirlo con el resto de extensiones cuyo comportamiento deseemos modificar.

29 IE 5.x/6.0 corta el margen izquierdo de la página al imprimirla

Básico



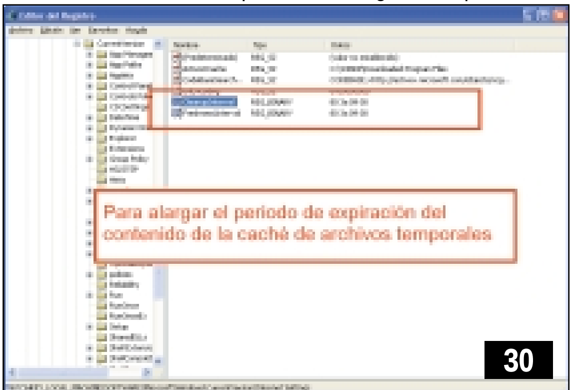
Si imprimimos una página web que contenga una tabla de datos cuyo tamaño sea mayor que el área imprimible de nuestro folio, la parte derecha de la tabla quedará cortada, y la segunda parte truncada no se imprimirá. Este es un comportamiento predeterminado de IE6, que únicamente puede ser resuelto reduciendo el tamaño de los márgenes bajo el menú *Archivo/imprimir* o imprimiendo la página con orientación horizontal.

Archivos temporales, Historial y Favoritos

30 Alargar el periodo de expiración de la memoria caché

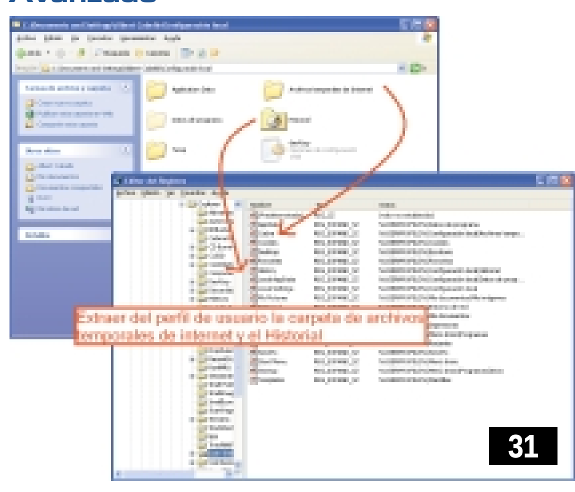
Avanzado

A menudo el contenido de la caché de archivos temporales expira demasiado pronto y los iconos, imágenes y páginas principales de las direcciones web no son mantenidos en la caché el tiempo que estimaríamos oportuno. Para modificar este comportamiento, iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache*. Allí crearemos o modificaremos el contenido del valor binario CleanupInterval y FreshnessInterval con el periodo en segundos que deseemos. El valor recomendado es sietes días (Valor 80 3A 09 00). Sin embargo, establecer un valor demasiado grande significará que nuestra caché aumentará en tamaño y podrá mostrar elementos ya caducados. Si nos podemos permitir ese gasto extra de espacio en disco, una caché más grande se traducirá en una navegación más rápida.



31 Mantener los *Archivos Temporales de Internet* y el *Historial* fuera del perfil de usuario

Avanzado

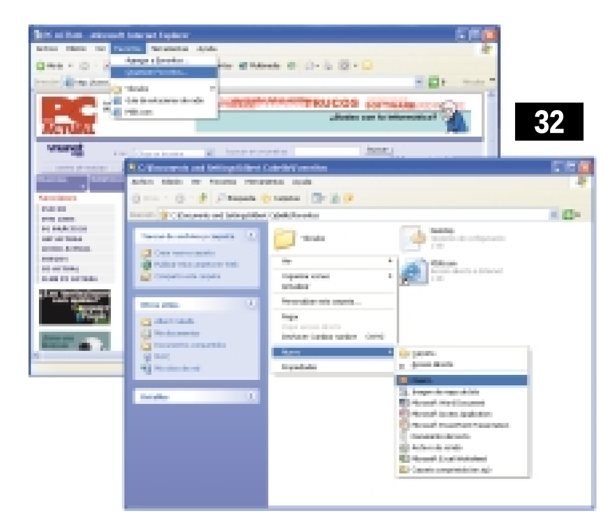


En sistemas NT-2000-XP, la carpeta de *Archivos Temporales de Internet* y el contenido del *Historial* se incluyen dentro de las carpetas que forman el perfil del usuario, de forma que cada usuario tiene sus propias carpetas independientes del resto. Sin embargo, esta característica ralentiza el inicio de sesión al arrancar el SO. Si queremos mantener ambas carpetas fuera del perfil de usuario y ubicarlas en cualquier sitio, incluso común para todos los usuarios, en primer lugar, iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejectuar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*. La entrada de tipo REG_SZ Cache determina la ubicación de la carpeta de *Archivos Temporales de Internet*, mientras que el valor de tipo REG_SZ History se refiere a la ubicación del *Historial*. Si estos valores existen también bajo la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders>,* deberemos realizar los cambios con la ruta completa de la nueva carpeta que almacenará estos datos.

32 Navegación móvil

Intermedio

Si navegamos por Internet desde un ordenador de sobremesa y un ordenador portátil al mismo tiempo, podemos utilizar la función *Maletín* de Windows para sincronizar nuestros favoritos entre ambos ordenadores. El *Maletín* nos permite sincronizar archivos concretos o carpetas enteras en nuestro portátil con los existentes en nuestro PC de sobremesa. Para ello, dentro de *Explorador* de Windows nos desplazaremos hasta la carpeta *\WINDIR\FAVORITOS* o *\DOCUMENTS AND SETTINGS\[NOMBRE_USUARIO\FAVORITOS* y haremos clic con el botón derecho del ratón sobre un área vacía en la lista de archivo. En el menú contextual que aparecerá, seleccionare-



mos *Nuevo/Maletín* y copiaremos este maletín a nuestra carpeta *Favoritos* en el equipo portátil utilizando para ello un disquete. Para usar este *Maletín*, cuando utilicemos la opción *Añadir a favoritos* para un enlace en una página Web, seleccionaremos la opción *Crear en* y nos trasladaremos hasta el *Maletín*. Cuando volvamos a nuestra oficina, utilizaremos el mismo disquete para sincronizar los archivos del *Maletín* con nuestro ordenador de sobremesa.

33 Acelerar *Favoritos* en Windows 2000-XP

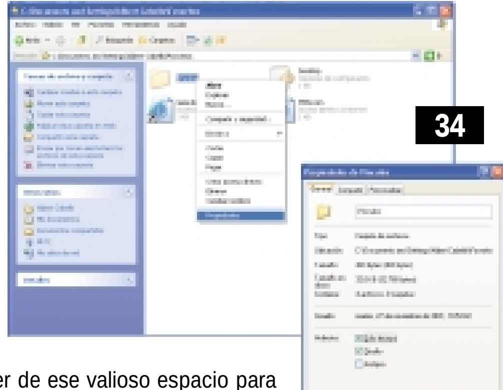
Intermedio

Por alguna extraña razón, el menú de *Favoritos* de Internet Explorer 6 parece funcionar de una manera muy lenta en ocasiones. Esto ocurre, por ejemplo, tras instalar TweakUI 1.33, cuando utilizamos una de las funciones que incluye para acelerar las animaciones del menú *Inicio*. Sin embargo, existe una solución a este problema que funciona, si bien no está claro por qué lo hace. Simplemente abriremos una ventana del intérprete de comandos desde el menú *Inicio/Programas/Accesorios/Intérprete de comandos* y ejecutaremos el verificador de archivos de sistema, introduciendo el comando «sfc.exe» con el parámetro */scannow*. Tras finalizar el proceso de verificación de archivos, nuestra carpeta de *Favoritos* se mostrará sensiblemente más rápida.

34 Ocultar la carpeta de *Vínculos*

Básico

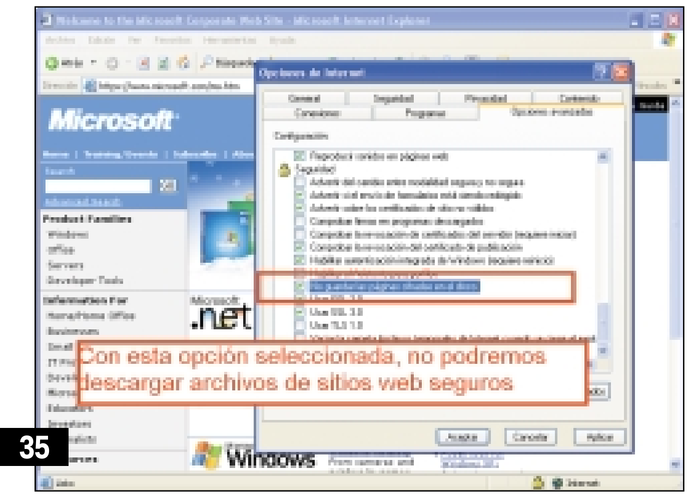
En muchas ocasiones la carpeta de enlaces de Internet Explorer funciona más como un sitio gratuito donde los fabricantes de software incluyen enlaces a los más variopintos sitios de la Red, dejando de lado su función original: disponer de un lugar donde almacenar los sitios más importantes a los que solemos acceder, para una rápida selección y carga. Para ocultar este menú y disponer de ese valioso espacio para otras *Barras de herramientas* o iconos, dentro del *Explorador* de Windows nos trasladaremos hasta la carpeta *C:\WINDIR\FAVORITOS* o *\DOCUMENTS AND SETTINGS\[NOMBRE_USUARIO \FAVORITOS*. Allí haremos clic con el botón derecho del ratón sobre la carpeta *Vínculos* y marcaremos en la pestaña *General* la marca de verificación sobre la casilla *Oculto*. Reiniciaremos el sistema par que los cambios surtan efecto.



Seguridad, asistente de contenidos y certificados digitales

35 Descargar archivos de sitios web seguros

Intermedio

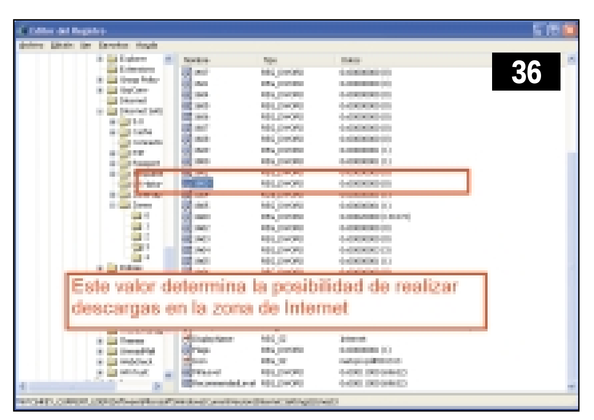


La opción *No guardar en disco las páginas encriptadas*, que encontraremos bajo la pestaña *Avanzada* dentro de las opciones de Internet, actúa en las páginas web de servidores seguros (por ejemplo, servicios de correo web) fácilmente localizables, ya que su URL comienza por *https://*, resultando útil en ordenadores compartidos donde queremos asegurarnos que nadie pueda acceder a estos datos sensibles (por ejemplo, números de tarjetas de crédito). Sin embargo, un fallo en el diseño de Internet Explorer puede provocar que cuando visitemos un sitio web seguro (*https://www.servidor.com/archivo.exe*) y tratemos de descargar o abrir un archivo, no aparezca el cuadro de diálogo para descargar en nuestro disco o ejecutar el archivo si hemos configurado, dentro de la pestaña *Avanzadas* del menú *Herramientas/opciones de Internet*, la opción *No guardar en disco las páginas encriptadas*, ya que ningún contenido de estas páginas podrá ser «cacheado» en la carpeta de *Archivos temporales de Internet,* y como no podrá «cachear» el archivo, no podrá abrirlo. Para solucionar el problema, desmarcaremos la casilla *Guardar en disco páginas encriptadas temporalmente* cuando vayamos a descargar un archivo de un servidor seguro.

36 Desactivar la función de descarga de archivos

Avanzado

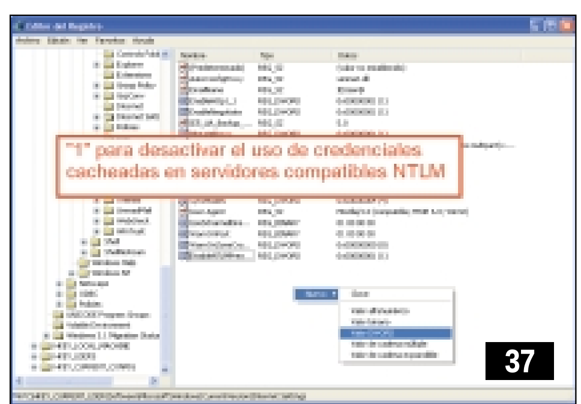
Mediante la edición del registro tenemos la posibilidad de desactivar la función de descarga de archivos, principal fuente de infección de virus en entornos de empresa y ordenadores públicos. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Ini-*



cio/Ejecutar y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3*. Allí crearemos o modificaremos valor DWORD 1803 cuyo contenido será 0 para permitir la descarga de archivos o 3 para deshabilitarla.

37 Desactivar el uso de la preautorización NTLM

Intermedio

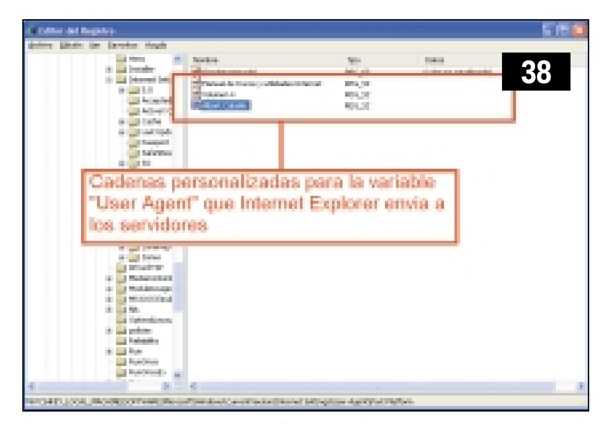


Con la versión 5.0 de Internet Explorer se incluyó una nueva función de preautorización NTLM que permite al navegador «cachear» las credenciales frente a servidores que utilicen este método de autenticación, de forma que las subsecuentes peticiones de autenticación utilicen las credenciales en la caché en vez de preguntar de nuevo al usuario su identificación y contraseña. No obstante, podemos desactivar esta funcionalidad iniciando la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizando la clave *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings*. Allí crearemos un nuevo valor DWORD o modificaremos el existente DisableNTLMPreAuth con el contenido 1 para desactivar esta característica o 0 para continuar haciendo uso de ella.

38 Modificar la cadena *User Agent* de Internet Explorer

Intermedio

Al utilizar el navegador para conectarnos a un servidor remoto, durante la conexión nuestro navegador envía al servidor una cadena *User Agent* que contiene detalles sobre el navegador cliente y el sistema operativo utilizado. Si bien esta información suele ser utilizada únicamente para fines estadísticos, podemos añadir, eliminar o modificar información de esta cadena.

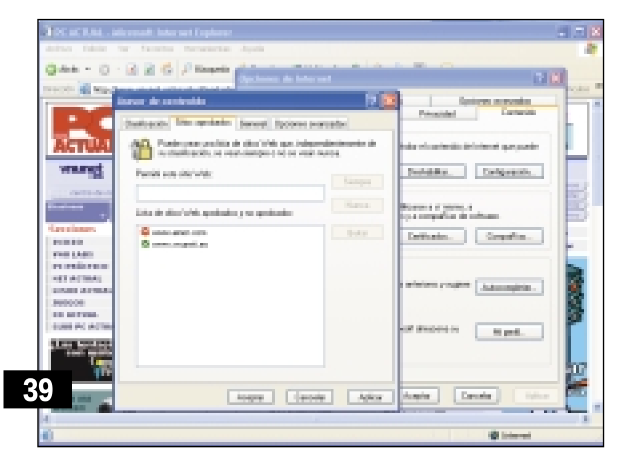


Una cadena *User Agent* estándar sería similar a:
Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0), que significa que estamos utilizando Internet Explorer 5.5 sobre un sistema Windows 2000.
Normalmente, una cadena *User Agent* personalizada podrá contener información adicional sobre la compañía que haya creado la versión personalizada del navegador, como por ejemplo:
Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; Nombre del ISP.
Debido a que esta información enviada a los servidores remotos puede ser almacenada en los archivos de registro del servidor y de esta forma usada posiblemente para localizar versiones modificadas del navegador, iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform*. Cada valor listado bajo esa clave representa una cadena adicional dentro de la cadena *User Agent* que será también enviada a los servidores remotos. Para eliminar toda información adicional, suprimiremos todas las entradas dentro de esta clave. Para añadir entradas adicionales, crearemos valores de tipo alfanumérico cuyo nombre será la cadena que queramos enviar. Deberemos reiniciar Internet Explorer para que los cambios surtan efecto.

39 Configurar la lista de sitios aprobados y no aprobados

Intermedio

Desde el menú *Herramientas/Opciones de Internet* en la pestaña *Contenido* tendremos acceso a la configuración del asistente de contenidos, cuya lista de sitios aprobados y no aprobados podremos configurar a nuestro gusto. Para ello, en

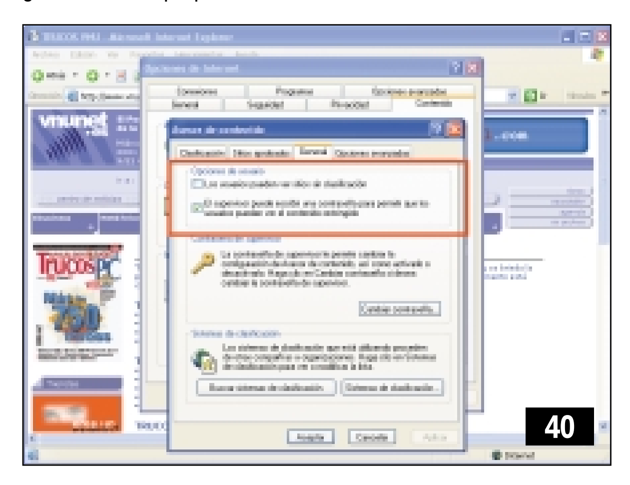


el área del *Asesor de contenidos* pulsaremos sobre el botón *Configuración* y, tras introducir la contraseña del supervisor, nos desplazaremos a la pestaña *Sitios aprobados*. Allí escribiremos las direcciones URL para cada sitio web a cuyo contenido los usuarios podrán o no acceder independientemente del nivel de clasificación establecido, y pulsaremos sobre los botones *Siempre* o *Nunca*. Para eliminar un sitio web aprobado o desaprobado, seleccionaremos la dirección URL de la lista y pulsaremos sobre el botón *Quitar*.

40 Configurar opciones de usuario

Intermedio

Para configurar las opciones de usuario para la calificación de contenidos dentro del menú *Herramientas/Opciones de Internet* en la pestaña *Contenido,* dentro del área del *Asesor de contenidos* accederemos a la *Configuración* tras introducir la contraseña del administrador. Seleccionaremos la pestaña *General* y en el área *Opciones de usuario* elegiremos la configuración más apropiada.

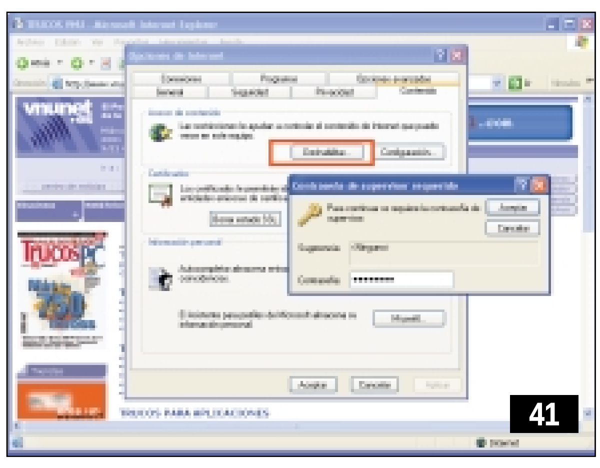


Los usuarios pueden ver sitios web sin calificación: seleccionaremos esta opción si queremos que los usuarios puedan acceder a páginas web cuyo contenido no se encuentre clasificado. *El supervisor puede escribir una contraseña para permitir que los usuarios puedan ver el contenido restringido*: seleccionaremos esta opción si queremos que los usuarios puedan acceder a páginas web con contenido restringido tras introducir la contraseña del supervisor.

41 Desactivar la configuración de seguridad

Intermedio

Si activamos la seguridad para evitar que algunos usuarios menores accedan a material no apto en Internet, resultará un suplicio tener siempre que introducir una contraseña para navegar por sitios web que contengan ese material. La mejor manera de evitar esa situación es deshabilitando temporalmente la configuración de seguridad mientras trabajamos. Para desactivar la seguridad, dentro del menú *Herramientas/Opciones de Internet* haremos clic en la pestaña *Contenidos*. Pulsaremos sobre el botón *Deshabilitar* e introduciremos la contraseña del administrador para configurar nuestra selección. Pulsaremos sobre *Aceptar* y también aceptaremos el cuadro de diálogo de advertencia, tras el que podremos navegar libremente por toda la Red. Sin embargo, no debemos olvidarnos de reactivar la configuración de seguridad antes de

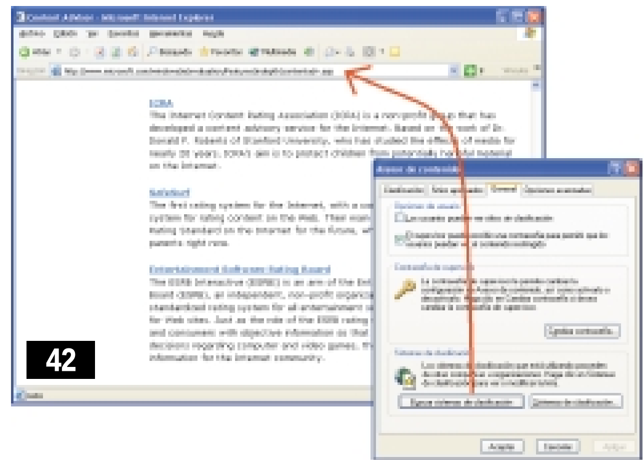


apagar el sistema. Estos ajustes permanecerán tal y como los teníamos anteriormente, de forma que sólo tendremos que introducir la contraseña para volver a aplicar las restricciones definidas con anterioridad.

42 Importar nuevos sistemas de calificación

Intermedio

Si bien en ocasiones puede ser necesario instalar con anterioridad algunos archivos de sistema o seguir las indicaciones proporcionadas por los servicios de calificación en sus respectivas páginas web, podemos importar nuevos sistemas de clasificación para los contenidos de las páginas en Internet Explorer. Para ello, dentro del menú *Herramientas/Opciones de Internet* en la pestaña *Contenido*, pulsaremos sobre el botón *Configuración* dentro del área del *Asesor de contenidos* y, tras introducir la contraseña de supervisor, nos desplazaremos hasta la pestaña *General*. Allí haremos clic en *Sistemas de clasificación* y seleccionaremos un sistema de clasificación alternativo de entre los existentes en la lista, o lo buscaremos en las carpetas de sistema de nuestro disco duro usando el botón *Añadir*, pulsando sobre *Aceptar* para aplicar los cambios.



Cabe señalar que podremos encontrar sistemas alternativos de clasificación de contenidos directamente desde el menú de *Opciones* del asesor de contenidos pulsando sobre el botón *Buscar sistemas de clasificación,* que nos conectará con el web *www.microsoft.com/windows/ie/evaluation/features/indepth/contentadv.asp,* donde podremos descargar los sistemas alternativos al estándar RSACi incluido en el navegador. Estos sistemas son ICRA, SafeSurf y Entertainment Software Rating Borad.

43 Asignar sitios a zonas de seguridad

Intermedio

Las siguientes tablas identifican los valores predeterminados para cada una de las opciones de configuración en las diferentes zonas de seguridad de Internet Explorer:

Autenticación de usuario

Opción de configuración	Baja	Media-Baja	Media	Alta
Inicio de sesión	Inicio de sesión automático con el nombre de usuario y contraseña actuales	Inicio de sesión automático sólo en la zona de intranet	Inicio de sesión anónimo	Preguntar por el nombre de usuario y la contraseña

Automatización

Opción de configuración	Baja	Media-Baja	Media	Alta
Secuencias de comandos activos	Activar	Activar	Activar	Desactivar
Permitir operaciones de pegado por medio de una secuencia de comandos	Activar	Activar	Activar	Desactivar
Automatización de los subprogramas de Java	Activar	Activar	Activar	Desactivar

Controles y complementos ActiveX

Opción de configuración	Baja	Media-Baja	Media	Alta
Descargar los controles firmados para ActiveX	Activar	Pedir datos	Pedir datos	Desactivar
Descargar los controles no firmados para ActiveX	Pedir datos	Desactivar	Desactivar	Desactivar
Inicializar y activar la secuencia de comandos de los controles de ActiveX no marcados como seguros	Pedir datos	Desactivar	Desactivar	Desactivar
Ejecutar controles y complementos de ActiveX	Activar	Activar	Activar	Desactivar
Activar la secuencia de comandos de los controles ActiveX marcados como seguros	Activar	Activar	Activar	Desactivar

Descargas

Opción de configuración	Baja	Media-Baja	Media	Alta
Descarga de archivos	Activar	Activar	Activar	Desactivar
Descarga de fuentes	Activar	Activar	Activar	Pedir datos

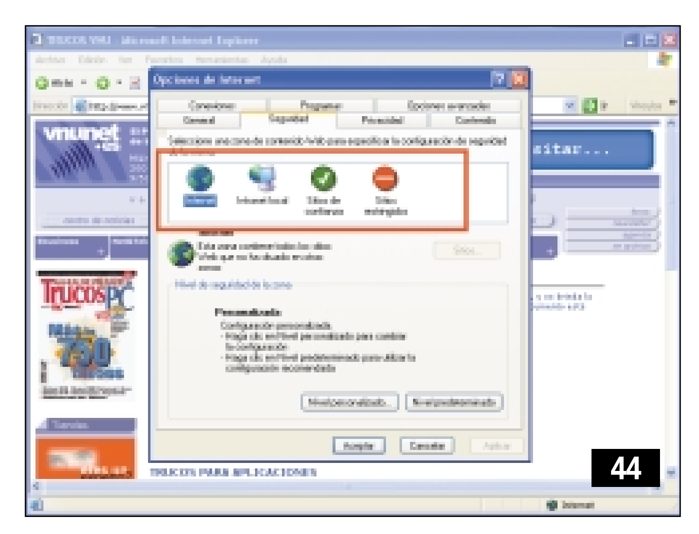
Miscelánea

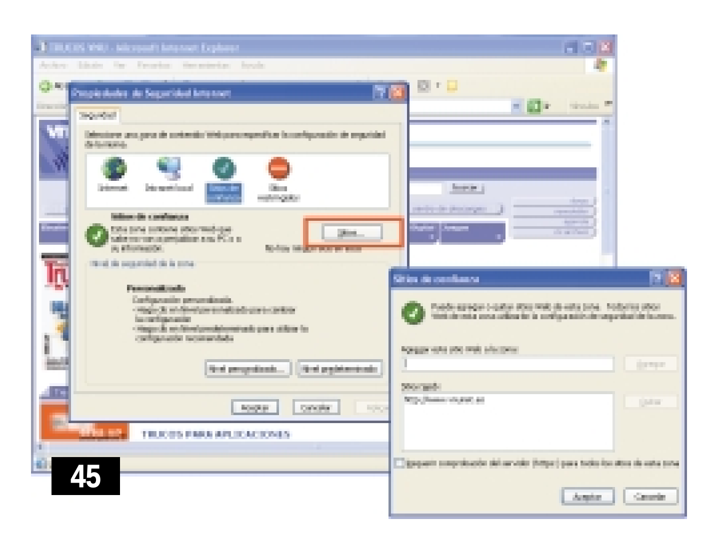
Opción de configuración	Baja	Media-Baja	Media	Alta
Tener acceso a origen de datos entre dominios	Activar	Pedir datos	Desactivar	Desactivar
Permitir Meta Actualizar	Activar	Activar	Activar	Desactivar
Mostrar contenido mixto	Pedir datos	Pedir datos	Pedir datos	Pedir datos
No pedir la selección del certificado de cliente cuando exista uno o ningún certificado	Activar	Activar	Desactivar	Desactivar
Arrastrar y colocar o copiar y pegar archivos	Activar	Activar	Activar	Pedir datos
Instalación de los componentes del Escritorio	Activar	Pedir datos	Pedir datos	Desactivar
Ejecutar programas y archivos en iframe	Activar	Pedir datos	Pedir datos	Desactivar
Desplazar subtramas a través de dominios distintos	Activar	Activar	Activar	Desactivar
Permisos de canal de software	Seguridad baja	Seguridad Media	Seguridad Media	Seguridad Alta
Enviar un formulario de datos no cifrados	Activar	Activar	Pedir datos	Pedir datos
Persistencia de los datos del usuario	Activar	Activar	Activar	Desactivar

44 Tipos de zonas de seguridad

Intermedio

Internet Explorer incluye cinco zonas de seguridad predefinidas:
Zona de intranet local: por defecto esta zona contiene todas las conexiones de red que hayan sido establecidas utilizando rutas UNC (*Universal Naming Convention*), por ejemplo *\\local\archivo.txt*, los sitios que no traspasen el servidor *proxy* o aquellos que tengan nombres que no incluyan puntos (por ejemplo, *http://local o file://C:*) y que no estén asignados a la zona de sitios restringidos o aprobados. El nivel de seguridad predeterminado para la zona de intranet local está establecido como medio (Internet Explorer 4.x) y medio-bajo (Internet Explorer 5 y superior).
Sitios de confianza: esta zona contiene los sitos web que están aprobados como seguros (como sitios web de la Intranet de nuestra empresa o compañías en las que tengamos confianza). Para añadir un sitio web a la zona de sitios aprobados, deberemos tener la certeza de que todos los archivos que descarguemos o ejecutemos desde ese sitio web no dañarán nuestro sistema o los datos en él contenidos. Por defecto no hay ningún sitio web asignado a la zona de sitios de confianza, y su nivel de seguridad está establecido como bajo.
Sitios restringidos: esta zona contiene los sitios web en los que





no confiamos. Cuando añadimos un sitio web a la zona de sitios restringidos, será porque tengamos la certeza de que los archivos que podamos descargar o ejecutar puedan hacer daño a nuestro sistema o los datos en él contenidos. Por defecto, no hay ningún sitio web asignado a la zona de sitios restringidos, y el nivel de seguridad está establecido como «Alto». La zona de sitios restringidos incluirá sitios web que no se encuentren en nuestro ordenador o intranet local, u otros que no hayan sido ya asignados a otra zona.
Internet: contiene los sitios web que no están en nuestro ordenador o intranet local o aquellos que no han sido asignados a otra zona. El nivel de seguridad predeterminado está establecido como medio.
Mi PC: esta zona (que contiene los archivos en nuestro ordenador local) únicamente puede personalizarse a través del Kit de Administración de Internet Explorer (IEAK), ya que no está disponible desde la interfaz del navegador. Los administradores deberán usar la configuración predeterminada para esta zona excepto si el entorno de trabajo tiene unos requerimientos específicos. Una configuración de seguridad baja puede tornarse en un riesgo de seguridad, y una configuración alta disminuir las funcionalidades del navegador.
Por defecto, la barra de estado del navegador mostrará un icono que nos informará de la zona cuya configuración se está aplicando dependiendo del sitio Web que por el que estemos navegando.

45 Asignar sitios a zonas de seguridad

Intermedio

Para cada zona de seguridad podemos asignar los sitios web que deseemos, y de esta manera se aplicará una configuración de seguridad del navegador diferente dependiendo del tipo de sitio por el que estemos navegando. Para añadir un sitio web a una zona de seguridad, dentro del menú *Herramientas/Opciones de Internet*, bajo la pestaña *Seguridad* o a través del icono existente en la barra de estado del navegador, haremos clic sobre la zona a la que queremos asignar un sitio Web y después pulsaremos sobre el botón *Sitios*. Si añadimos un sitio web a la zona de intranet local, podemos seleccionar los tipos de sitios web que queramos incluir en la zona y después pulsar sobre *Avanzada* para añadir sitios específicos. Las siguientes reglas se aplican a las opciones de la zona de intranet local. Sin embargo, hemos de tener en cuenta que asignar un sitio web a una zona tendrá preferencia sobre las reglas generales.

Es conveniente recordar que no podemos asignar un sitio web a la zona de Internet, porque esta zona contiene todos los sitios web que no están en nuestro ordenador, en la zona de la intranet local o aquellos que no estén asignados ya a otra zona.

46 Instalar y eliminar certificados aprobados

Intermedio

El administrador de certificados de Internet Explorer nos permite instalar y eliminar certificados aprobados con anterioridad. Estos certificados pueden ser utilizados para autenticar a clientes, asegurar el correo electrónico u otras opciones más avanzadas. Para instalar y eliminar clientes y autoridades certificadoras de la lista de certificados aprobados, podemos utilizar el Administrador de certificados de Internet Explorer dentro del menú *Herramientas/Opciones de internet* pulsando sobre la pestaña *Contenido* y allí sobre el botón *Certificados*. Pulsaremos sobre una de las categorías para los diferentes tipos de certificados que queramos instalar y finalmente sobre el botón *Importar*, siguiendo los pasos del asistente que aparecerá. Para *Exportar* certificados, el asistente para la exportación de certificados también nos guiará durante el proceso de exportación.



También podremos eliminar un certificado existente de la lista de certificados de confianza pulsando sobre *Eliminar*, y *Ver* las propiedades de un certificado seleccionado, incluyendo el emisor del certificado y sus fechas de validez.

47 Tipos de certificados

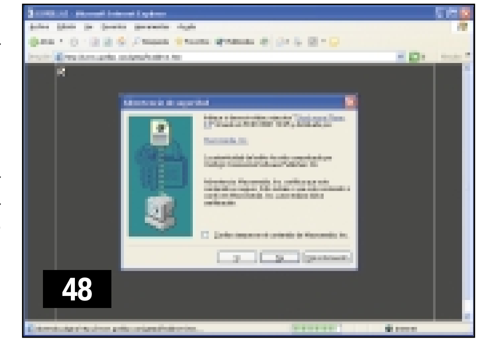
Básico

En caso de que queramos administrar la lista de certificados o eliminar certificados anteriormente aprobados, dentro del mismo menú *Herramientas/Opciones de Internet* pulsando sobre la pestaña *Contenido* y después sobre el botón *Certificados,* seleccionaremos una de las categorías para los diferentes tipos de certificados y la configuraremos. Estas categorías son:
Personal: los certificados en la categoría *Personal* utilizarán una clave privada asociada a ellos. La información firmada con certificados personales se identificará con los datos de la clave privada del usuario. Por defecto, Internet Explorer almacenará todos los certificados que identifiquen al usuario (con una clave privada) en la categoría *Personal*.
Otras personas: los certificados en esta categoría utilizarán una clave pública criptográfica para autenticar su identidad, basada en una clave privada de cifrado que se utilizará para firmar la información. Por defecto esta categoría incluirá todos los certificados que no estén en la categoría *Personal* (no tendrán clave privada para identificar al usuario) y que no pertenezcan a una entidad emisora de certificados.
Entidades emisoras de certificados intermedias: esta categoría contiene todos los certificados para las entidades emisoras que no sean entidades emisoras raíz.
Entidades emisoras raíz de confianza: esta categoría incluirá certificados semi-firmados en la carpeta raíz. Cuando una entidad emisora raíz de certificados esté listada en esta categoría, nosotros configuraremos los contenidos de los sitios, personas y emisores con credenciales proporcionadas por la entidad emisora
Editores de confianza: esta categoría contendrá únicamente los certificados de los editores de confianza cuyo contenido puede ser descargado sin la intervención del usuario. Dentro del cuadro de diálogo *Propósitos planteados del certificado*, seleccionaremos el filtro para los tipos de certificados que queremos mostrar en la lista.

48 Añadir editores de confianza

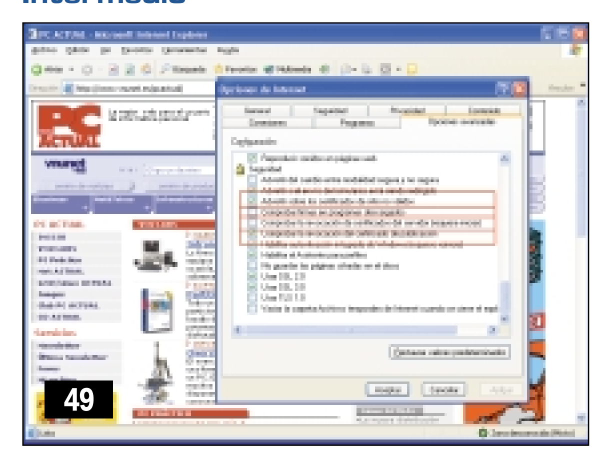
Intermedio

Para designar un editor de confianza para Internet Explorer, utilizaremos el cuadro de diálogo de advertencia de seguridad que aparecerá cuando intentemos descargar software de un editor. En este cuadro de diálogo, marcaremos la casilla *Confiar siempre en contenido de…*, tras lo que se descargará el software, se instalarán los controles apropiados y se añadirá el editor del control a la lista de editores de confianza. Una vez hecho esto, el contenido activo que está digitalmente firmado por los editores de confianza con un certificado válido se descargará sin la intervención del usuario, a excepción de que hayamos desactivado la descarga de contenido activo en la configuración de una zona de seguridad específica.



49 Configurar opciones avanzadas de seguridad para certificados y características de autenticación

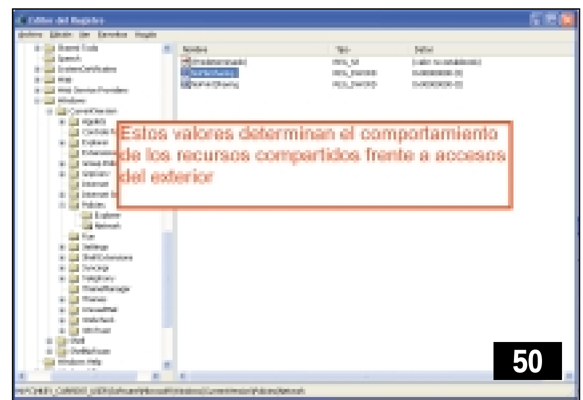
Intermedio



Podemos configurar fácilmente las opciones para los certificados y las características de autenticación que nuestros usuarios utilizarán desde el menú *Herramientas/Opciones de Internet*, bajo la pestaña *Configuración Avanzada,* en el apartado *Seguridad*. Dependiendo del nivel de seguridad que necesitemos, marcaremos o desmarcaremos las casillas de verificación existentes: *Advertir sobre los certificados de sitio no válidos*, *Comprobar firmas en programas descargados*, *Comprobar la revocación de certificados del servidor* y *Comprobar la revocación del certificado de publicación*.

50 Aumentar la seguridad en conexiones permanentes a Internet

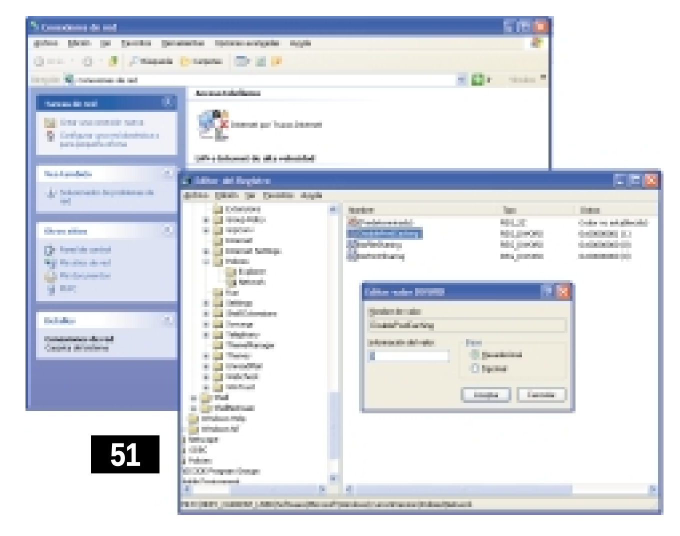
Avanzado



Con la proliferación del acceso a Internet a través de las líneas ADSL, toda medida para aumentar la seguridad en nuestro sistema siempre es bienvenida. Entre ellas, especialmente importante es la compartición de archivos e impresoras, cuya administración podemos desactivar modificando un valor en el registro. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network*. Allí añadiremos o modificaremos los valores DWORD existentes NoFileSharing y NoPrintSharing con el contenido 0 para no compartir elementos a través de las redes o 1 para continuar compartiendo elementos.

51 Qué hacer si la casilla *Recordar contraseña* en conexiones a Internet está sombreada

Intermedio



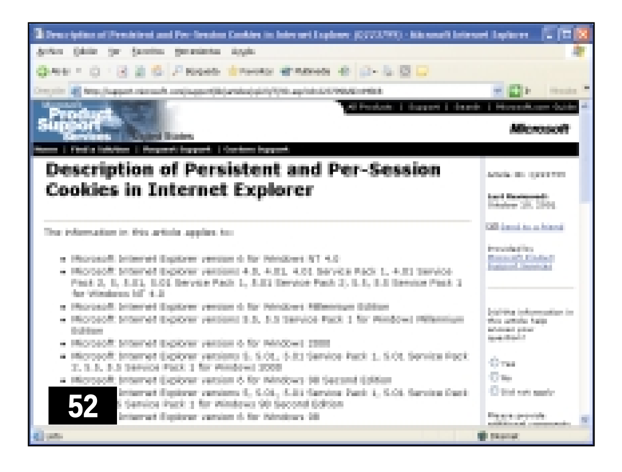
Si al ejecutar una conexión de acceso telefónico a redes en equipos 9x-Me encontramos sombreada la opción que nos permite recordar nuestra contraseña, todavía podremos intentar revertir este comportamiento antes de reinstalar el sistema. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network*. Allí nos aseguraremos que, de existir el valor DWORD DisablePwdCaching, su contenido sea 0.

Cookies y privacidad

52 *Cookies* permanentes vs. *cookies* de sesión

Intermedio

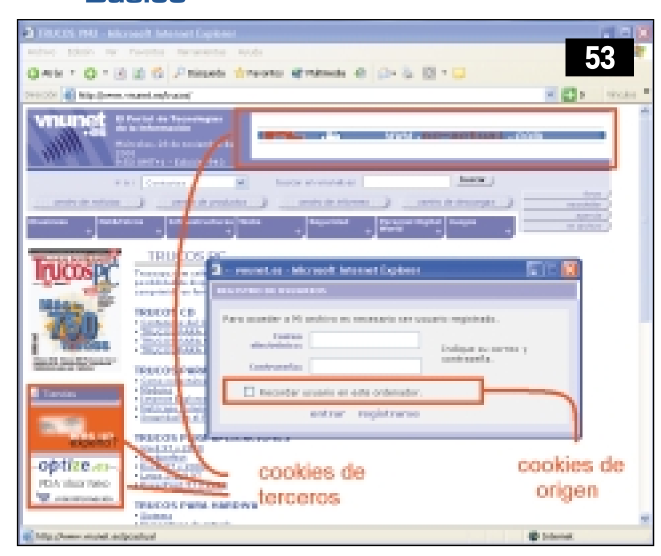
Existen dos tipos de *cookies*. Las permanentes son usadas para almacenar información sobre las visitas a un sitio Web y están dentro de la carpeta *DOCUMENTS AND SETTINGS\[NOMBRE_USAURIO\COOKIES* o en la carpeta *WINDIR\COOKIES* por un periodo de tiempo definido por el servidor Web cuando



se utiliza Internet Explorer. El segundo tipo son las *cookies* de sesión, utilizadas para guardar información únicamente durante la sesión de navegación de un usuario en un sitio web. Estas *cookies* son «cacheadas» en memoria únicamente mientras el usuario está visitando el servidor Web, tras lo que se obtiene una *cookie* de sesión, y son eliminadas de la caché cuando el usuario cierra la sesión. Para desactivar el uso de las *cookies* de sesión, dentro de la pestaña *Privacidad* pulsaremos sobre el botón *Opciones avanzadas* y nos aseguraremos de que la casilla *Aceptar siempre las cookies de sesión* esté activada. De esta forma, las *cookies* de sesión se almacenarán de forma temporal hasta que cerremos todas las ventanas del explorador. Para más información sobre las *cookies* permanentes y de sesión, el articulo Q223799 de la *Knowledge* base de Microsoft nos ayudará.
NOTA: Las versiones 3.x y 4.x de Internet Explorer no distinguen entre *cookies* permanentes y de sesión.

53 *Cookies* de origen vs. *cookies* de terceros

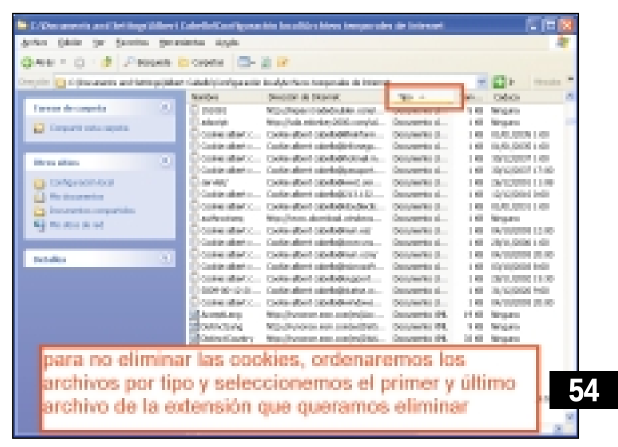
Básico



Las *cookies* de origen son aquellas que están asociadas con el servidor de dominio con el que pretendemos conectar, mientras que las *cookies* de terceros pertenecerán a otro dominio. Por ejemplo, supongamos que visitamos *www.ejemplo1.com* y *muestra.ejemplo1.com* escribiendo la URL en la barra de direcciones, y más tarde *www.ejemplo1.net* que contiene un *banner* publicitario en la página. Si todos estos sitios web han almacenado *cookies* en nuestro ordenador, las *cookies* de los sitios *www.ejemplo1.com* y *muestra.ejemplo1.com* podremos definirlas como *cookies* de origen, mientras que las *cookies* de *www.ejemplo1.net* serán de terceros.
Si visitamos *www.ejemplo1.com* bajo una conexión segura usando el protocolo HTTPS (*Secure Hypertext Transfer Protocol*), el contenido en esa página que no esté utilizando el protocolo HTTPS se considerará como contenido de terceros. También tendremos en cuenta que si accedemos a un sitio que usa *cookies* utilizando marcos o portales en otro sitio web, estas *cookies* se considerarán de terceros. Las *cookies* son asignadas únicamente a nuestro perfil de usuario y sólo pueden ser leídas por el servidor de dominio que nos la proporcionó. A excepción de Internet Explorer 6.0 y la versión *Advanced Security Privacy Beta* de Internet Explorer 5.5 (Version 5.50.4308.2900), Internet Explorer 3.x, 4.x, 5, 5.01 y 5.5 no distinguen entre *cookies* de origen y de terceros.

54 Cómo eliminar archivos temporales de Internet sin borrar las *cookies*

Básico

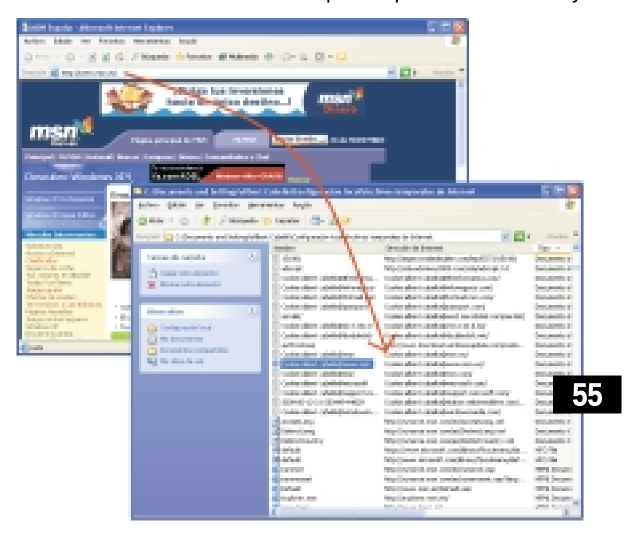


Si decidimos purgar por completo el contenido de la caché de Internet Explorer (situada normalmente en el directorio *\WINDIR\ARCHIVOS TEMPORALES DE INTERNET* o *\DOCUMENTS AND SETTINGS\[NOMBRE_USUARIO\DATOS DE PROGRAMA\ARCHIVOS TEMPORALES DE INTERNET*, podemos hacerlo sin necesidad de eliminar las *cookies*. En primer lugar ordenaremos los iconos por tipo, pulsaremos en el primer archivo con extensión «.htm*» y bajaremos hasta el último, donde lo seleccionaremos mientras mantenemos pulsada la tecla «Mayúsculas». Tras pulsar «Suprimir», eliminaremos todos los archivos comprendidos entre los dos seleccionados pero manteniendo intactas nuestras *cookies* y nuestras opciones de configuración y preferencias en multitud de sitios web. Tendremos que realizar estos pasos para cada tipo de archivo que queramos eliminar de la caché de archivos temporales de Internet.

55 Cómo eliminar una *cookie*

Intermedio

Como ya sabréis, las *cookies* contienen información sobre una visita realizada anteriormente a un sitio web. Para eliminar una *cookie* concreta iniciaremos Internet Explorer. Dentro del menú *Herramientas* seleccionaremos la opción *Opciones de Internet* y

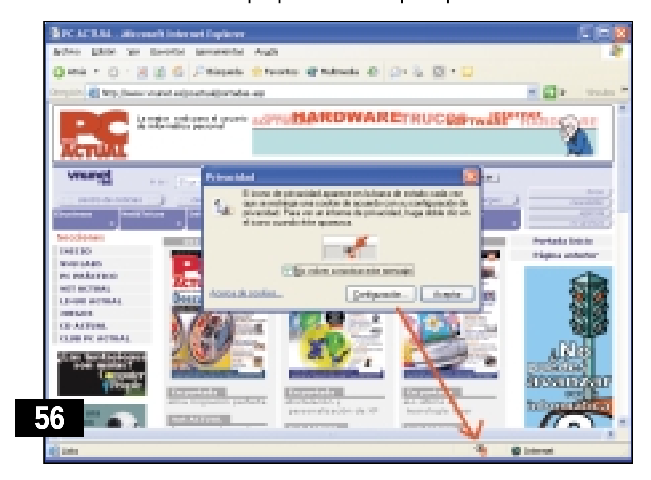


la pestaña *General*, donde pulsaremos sobre el botón *Configuración* que encontraremos bajo el apartado *Archivos temporales de Internet*. Tras pulsar sobre el botón *Ver archivos*, nos aseguraremos de que esté seleccionada la vista *Detalles* en el menú *Ver* y haremos clic sobre la cabecera de la columna *Dirección de Internet* para organizar las *cookies*, que tendrán un formato *cookie:[nombre_usuario]@[servidor_web.com]*. Una vez localizada, seleccionaremos el archivo y pulsaremos sobre la tecla «Suprimir» en nuestro teclado. Confirmaremos la eliminación respondiendo «Sí» en caso de ser preguntados.

56 Cómo gestionar la privacidad de Internet Explorer

Intermedio

Una de las características más importantes del nuevo Internet Explorer 6.0 es la administración personalizada de *cookies*, cuya configuración se encuentra dentro del menú *Herramientas/Opciones de Internet* bajo la pestaña *Privacidad* o haciendo doble clic en el pequeño icono que aparecerá en la barra

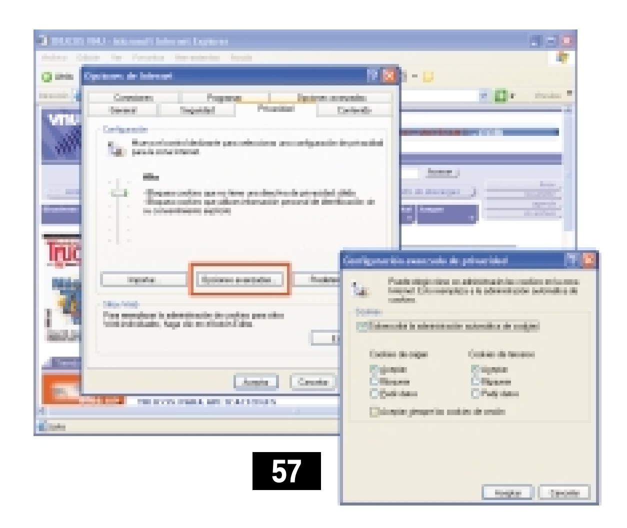


de estado de nuestro navegador al entrar en una página web cuya política de privacidad no esté definida. En este panel, cuya configuración afectará únicamente a la zona Internet definida en el navegador, personalizaremos el nivel de intimidad que queramos durante nuestra navegación escogiendo entre las seis configuraciones estándar distintas de privacidad existentes (*Bloquear todas las cookies, Alta, Media-Alta, Media, Baja y Aceptar todas las cookies*). De esta manera, especificaremos cómo utilizarán nuestros datos personales los sitios web por los que naveguemos a través de las *cookies*, incluyendo las páginas que hemos visto y el tipo de navegador que hemos utilizado, entre otros datos.

57 Configuración avanzada de privacidad

Intermedio

Tras seleccionar una de las seis configuraciones estándar, pulsando sobre el botón *Opciones avanzadas* aparecerá un nuevo cuadro con las características de la configuración seleccionada. En estos ajustes comprobaremos el modo en que el navegador diferencia entre las *cookies* originadas por sitios web que proporcionan servicios de publicidad (*cookies* de terceros), de las generadas intencionadamente por el servidor que aloja la página Web (*cookies* de origen) para personalizar nuestros contenidos, recordar nuestro nombre de usuario y

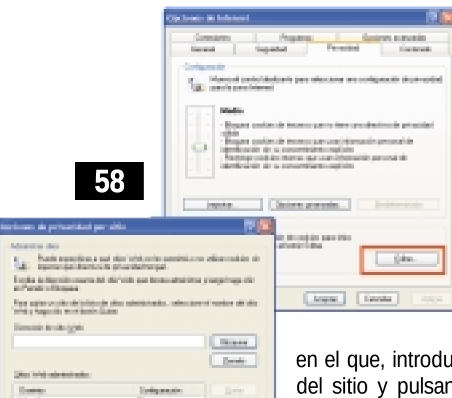

57

contraseña, etc. Para cada uno de estos dos valores podremos optar entre *Bloquear*, *Aceptar* todas o preguntar (*Pedir datos*) para cada una de las *cookies* que ambos tipos de sitios web a los que accedamos nos envíen. Esta última opción consumirá gran parte de nuestro tiempo si visitamos bastantes sitios web, por lo que no aconsejamos su utilización. También es importante destacar que muchos sitios web no funcionarán correctamente si desactivamos el uso de *cookies* de origen, y que desactivando las *cookies* de terceros no se mostrarán la mayoría de *banners* publicitarios.

58 Privacidad personalizada

Intermedio

Sin embargo, los usuarios más exigentes con el control y personalización de su experiencia de navegación podrán incluso definir una política de privacidad muy estricta y especificar individualmente el nombre de aquellos sitios web para los que se ignorará la política global de privacidad definida anteriormente y se permitirá o prohibirá terminantemente el uso de las *cookies*. Pulsando sobre el botón *Editar* dentro de la pestaña *Privacidad* que encontraremos bajo el menú *Herramientas/Opciones de Internet*, aparecerá un nuevo cuadro de diálogo en el que, introduciendo la dirección web exacta del sitio y pulsando sobre el botón *Bloquear* o *Permitir,* estableceremos la configuración especial para esos sitios web. Esta lista puede ser modificada en cualquier momento, eliminando o añadiendo nuevas entradas.


58

59 Niveles de privacidad, a fondo

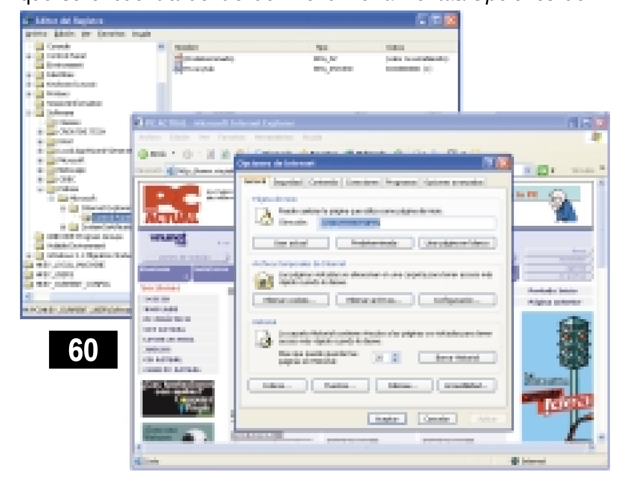
Intermedio

Seleccionar esto	Para obtener este resultado
Bloquear todas las *cookies*	Internet Explorer evitará que los sitios web almacenen *cookies* en nuestro ordenador y los sitios web tampoco podrán leer las *cookies* existentes en nuestro ordenador.
Alta	Internet Explorer evitará que los sitios web almacenen *cookies* que no tengan una política compacta de privacidad (un manifiesto de privacidad resumido inteligible entre ordenadores). El navegador también evitará que los sitios web almacenen *cookies* que usen información que pueda identificarnos personalmente sin nuestro consentimiento explícito. Las *cookies* que estuvieran en nuestro ordenador antes de instalar Internet Explorer 6 serán restringidas, de forma que sólo puedan ser leídas por el servidor Web que las originó.
Media Alta	Internet Explorer evitará que los sitios web almacenen *cookies* de terceros que no tengan una política compacta de privacidad o que usen información que pueda identificarnos personalmente sin nuestro consentimiento. El navegador también evitará que los sitios web almacenen *cookies* de origen que usen información que puedan identificarnos personalmente sin nuestro consentimiento implícito. Las *cookies* de origen que no tengan una política compacta de privacidad y aquellas que ya estuvieran en nuestro ordenador antes de instalar IE6 serán restringidas, de modo que únicamente puedan ser leídas en por el servidor Web que las originó
Media (nivel predeterminado)	Internet Explorer evitará que los sitios web almacenen *cookies* de terceros que no tengan una política compacta de privacidad o que hagan uso de información que pueda identificarnos personalmente sin nuestro consentimiento implícito. El navegador permitirá *cookies* de origen que incluyan información que pueda identificarnos personalmente sin nuestro consentimiento implícito, pero las eliminará cuando cerremos el navegador. Las *cookies* de origen que no tengan una política compacta de privacidad, así como las existentes en nuestro ordenador antes de instalar IE6, serán restringidas y sólo podrán ser leídas por el servidor Web que las originó.
Baja	Internet Explorer permitirá que los sitios web almacenen *cookies* en nuestro sistema, incluyendo *cookies* de terceros que no tengan una política compacta de privacidad o que hagan uso de información que pueda identificarnos personalmente sin nuestro consentimiento implícito. Sin embargo, cuando cerremos el navegador, se eliminarán todas las *cookies* de terceros de nuestro ordenador. Las cookies de origen que no tengan una política compacta de privacidad, así como las existentes en nuestro ordenador antes de instalar IE6, serán restringidas, de forma que sólo puedan ser leídas por el servidor que las originó
Aceptar todas las *cookies*	Internet Explorer permitirá que todos los sitios web almacenen *cookies* en nuestro sistema y las *cookies* existentes en nuestro sistema podrán ser leídas por los sitios web que las crearon sin ninguna restricción.

60 Eliminar la pestaña *Privacidad*

Intermedio

Utilizaremos este truco para desactivar la pestaña *Privacidad* que se encuentra dentro del menú *Herramientas/Opciones de*

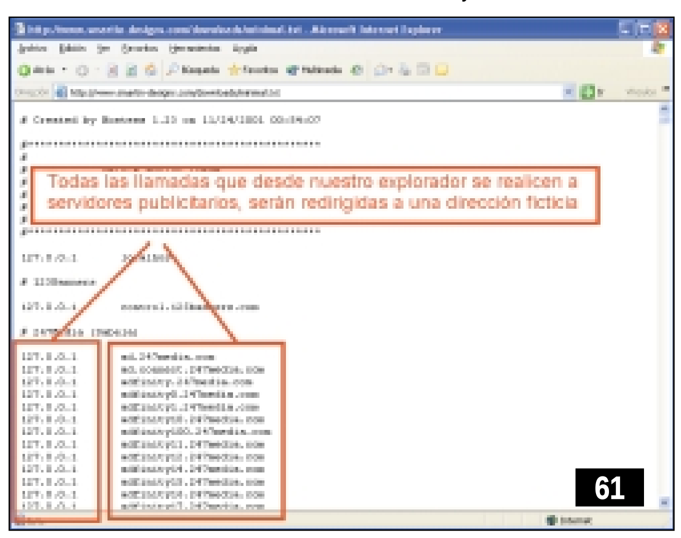


Internet de Internet Explorer 6.0. Iniciaremos el editor del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel*. Allí crearemos o modificaremos el valor DWORD Privacytab cuyo contenido será 1 para ocultar su acceso o 0 para continuar mostrándolo.

61 Otra forma de bloquear publicidad

Avanzado

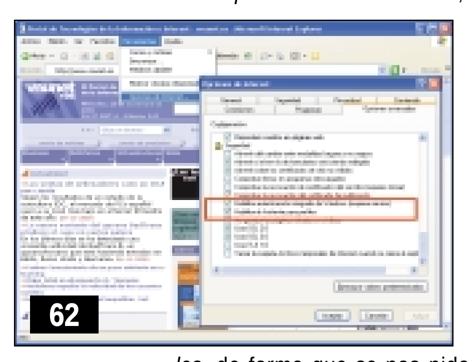
Una forma diferente de bloquear los *banners* publicitarios es utilizando un archivo de *hosts*. Éste se encarga de traducir a direcciones IP los nombres DNS de servidores web. Trasladando su función a nuestro truco, este archivo se encargará de que nuestra máquina no pueda acceder a los servidores de publicidad en él especificados a través de Internet, redirigiendo las llamadas a servidores de publicidad a una dirección ficticia o dentro de la red local. Este archivo «hosts.» tendremos que copiarlo en el directorio *\WINDOWS* si utilizamos Windows 9x-Me o *C:\WINDOWS\SYSTEM32\DRIVERS\ETC* si utilizamos Windows NT-2000-XP, y mantenerlo actualizado, ya que cada día aparecen nuevos servicios de publicidad en la Red. Podréis encontrar más información, así como versiones frecuentemente actualizadas de este archivo, en el web *www.smartin-designs.com*. Conviene tener en cuenta que cualquier entrada existente en el archivo «hosts.» no será accesible desde el navegador, y esta podrá ser la causa de que algunas páginas no se muestren correctamente.



62 Configurar el *Asistente de perfiles*

Intermedio

El *Asistente de perfiles* almacena nuestro perfil de usuario, que contiene la información que compartiremos con los sitios web. Otros programas de Internet, incluyendo NetMeeting y Outlook Express, también hacen uso del *Asistente de perfiles*. De esta forma, cuando un sitio web realice una solicitud de información sobre nosotros, aparecerá dicho asistente que nos pedirá confirmación y los datos que compartiremos con el servidor web. En el menú *Herramientas/Opciones de Internet*, dentro de la pestaña *Avanzada* y bajo el apartado *Seguridad*, dependiendo de nuestras necesidades marcaremos la casilla *Habilitar el asistente para perfiles,* de forma que se nos pida consentimiento para que el asistente envíe información a los sitios web, o la desmarcaremos para directamente no permitir el envío de esta información ante las solicitudes

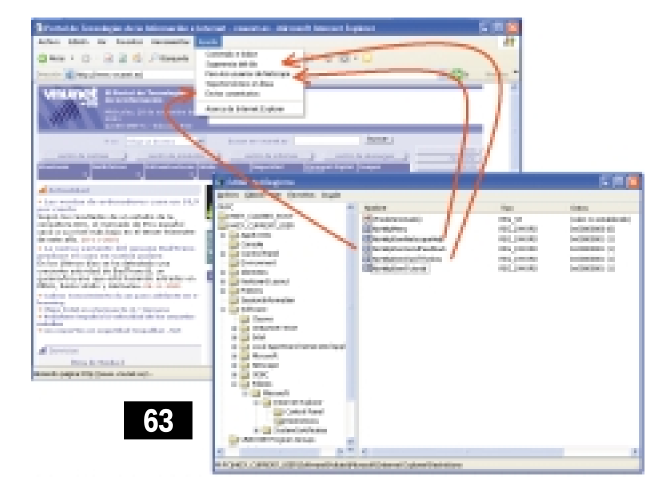


Restricciones

63 Restringir los menús de ayuda

Intermedio

Cada uno de los elementos del menú de *Ayuda* de Internet Explorer pueden ser ocultados individualmente o desactivado por completo el citado menú. Para ello, iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet*



Explorer\Restrictions. Allí crearemos un nuevo valor DWORD, cuyo contenido será 1 para activar la restricción y ocultar por tanto el acceso o 0 para desactivarla y continuar mostrándolo.
NoHelpMenu oculta por completo el menú de ayuda.
NoHelpItemNetscapeHelp oculta el elemento de ayuda para usuarios de Netscape Navigator.
NoHelpItemSendFeedback oculta el elemento enviar comentarios.
NoHelpItemTipOfTheDay oculta el elemento sugerencia del día.
NoHelpItemTutorial oculta el elemento Tour (Tutorial) del navegador (únicamente en IE 4.x).

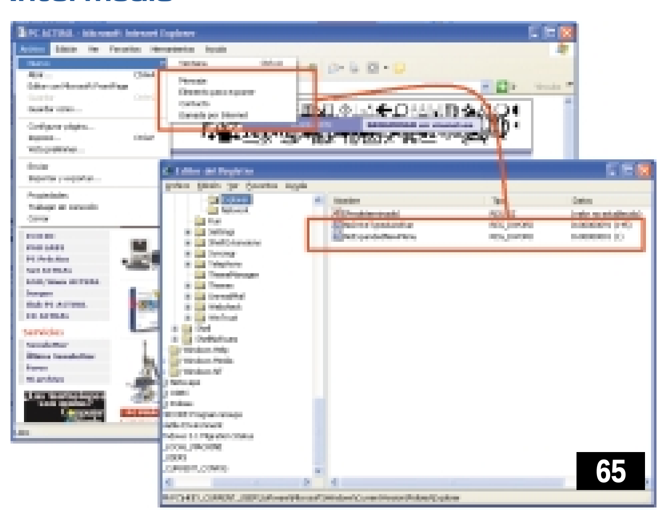
64 ¿Tenemos deshabilitado el asistente de conexión a Internet?

Intermedio

Si una política de seguridad definida por el administrador de sistema en equipos NT-2000-XP nos prohíbe la ejecución del asistente de conexión a Internet, podemos utilizar la herramienta de edición del registro para solucionar el problema. Ejecutaremos la aplicación con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel*. Allí eliminaremos, en caso de existir, el valor DWORD Connwiz Admin Lock.

65 Desactivar las opciones extendidas del menú *Nuevo*

Intermedio



Normalmente, cuando hacemos clic en el submenú *Nuevo* que encontramos dentro del menú *Archivo* en la ventana principal del navegador, Internet Explorer nos muestra varias opciones tales como *Nueva ventana, mensaje, elemento para exponer y llamada de Internet*. Mediante la edición del registro podemos evitar que se muestren las opciones extendidas de este menú y que únicamente se vea la opción *Nueva Ventana*. Para ello iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*. Allí crearemos o modificaremos el valor DWORD existente NoExpandedNewMenu, cuyo contenido será 1 para evitar que se vean las opciones extendidas del menú y 0 para continuar mostrándolas.

66 Evitar que los usuarios de NT-2000-XP usen la función *Establecer como papel tapiz*

Intermedio

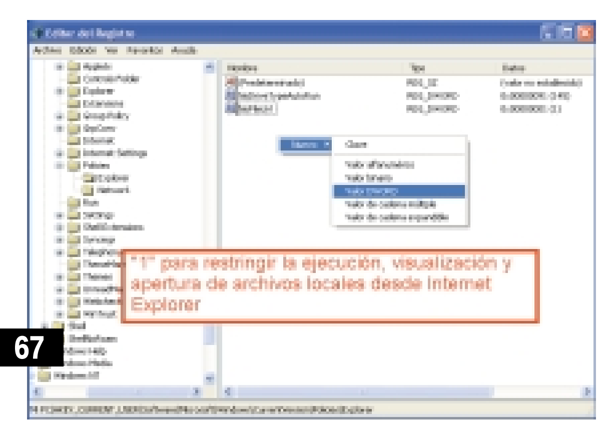
Cuando un usuario hace clic con el botón derecho del ratón sobre una imagen dentro de Internet Explorer y selecciona la opción *Establecer como papel tapiz*, se crea un archivo «Internet Explorer Wallpaper.bmp» dentro de la carpeta *\DOCUMENTS AND SETTINGS\%USERNAME%\APPLICATION DATA\MICROSOFT\INTERNET EXPLORER*. Para evitar esta acción, y que los usuarios no puedan utilizar esta función de Internet Explorer para modificar el papel tapiz de su *Escritorio*, utilizaremos IE para establecer nosotros el papel tapiz que deseemos. Copiaremos el archivo «Internet Explorer wallpaper.bmp» resultante dentro de la carpeta *\DOCUMENTS AND SETTINGS\%USERNAME%\APPLICATION DATA\MICROSOFT\INTERNET EXPLORER* de todos los usuarios a los que queramos inhibir esta posibilidad y estableceremos los permisos de este archivo para permitir únicamente su lectura y no su escritura o modificación. Para ello utilizaremos la siguiente orden dentro de una ventana del intérprete de comandos:
CACLS "%userprofile%\Application Data\Microsoft\Internet Explorer\Internet Explorer Wallpaper.bmp" /g SYSTEM:F Administrator:F Everyone:R
Cabe señalar que este truco sólo funcionará cuando el perfil de usuario se encuentre almacenado en una partición que utilice NTFS como sistema de archivos.

66

67 Limitar el acceso a unidades locales desde Internet Explorer

Avanzado

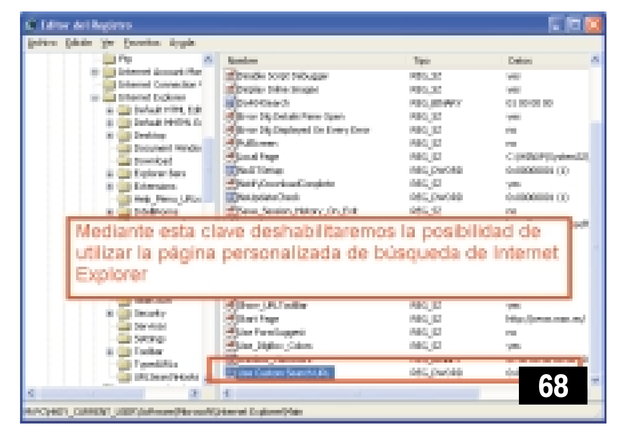
Internet Explorer permite la ejecución, visualización y apertura de archivos locales ubicados en las unidades de sistema si escribimos en la *Barra de direcciones* la ruta donde se encuentra el archivo o su URL (*file://c:\...*). No obstante, podemos establecer una restricción que limite el acceso a los archivos locales de sistema desde el navegador. Para ello, iniciaremos la herramienta de edición del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la



clave HKEY_CURRENT_USER\Software\Microsoft\Windows\-CurrentVersion\Policies\Explorer. Allí crearemos un valor DWORD o modificaremos el existente NoFileUrl cuyo contenido será 1 para evitar el uso de la sintaxis *file://c:\...* en la *Barra de direcciones* o 0 para poder continuar utilizando Internet Explorer para abrir archivos locales

68 Desactivar la página personalizada de búsqueda

Intermedio

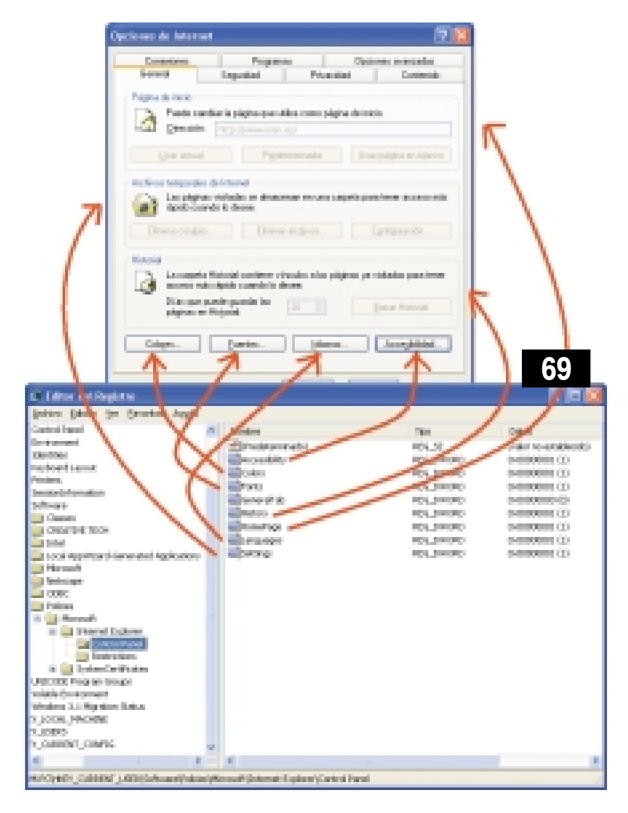


Mediante la edición del registro de Windows podremos deshabilitar la posibilidad de utilizar la página personalizada de búsqueda de Internet Explorer. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main*. Allí crearemos un nuevo valor DWORD o modificaremos el existente Use Custom Search URL, cuyo contenido será 1 para continuar utilizando la página personalizada de búsqueda o 0 para deshabilitar esta función.

69 Restricciones en el *Panel de control* de Internet Explorer

Avanzado

Con este truco podremos controlar el acceso a muchos de los aspectos de configuración de Internet Explorer y otras funciones del *Panel de control* para la aplicación, que podemos encontrar bajo el menú *Herramientas/Opciones de internet* en la pantalla principal del navegador. Abriremos el editor de registro con el comando «regedit.exe» en el menú *Inicio/Ejecutar*, localizaremos la clave *HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel* y crearemos un nuevo valor DWORD basado en las opciones siguiente con el valor 1 para activar la restricción o 0 para desactivarla.
GeneralTab desactiva la pestaña *General*.
HomePage desactiva el cuadro *Página de Inicio*.
Settings desactiva la configuración de la carpeta *Archivos Temporales de Internet*.
History desactiva la configuración del *Historial de navegación.*
Colors desactiva la configuración de los *Colores* de fondo, texto y enlaces.
Fonts desactiva la configuración de las *fuentes* con las que se mostrarán las páginas web.
Languages desactiva el botón de configuración de lenguajes.
Accessibility desactiva el botón *Accesibilidad* de la pestaña *General*.
SecurityTab desactiva la pestaña *Seguridad*.



SecChangeSettings desactiva la modificación de niveles de seguridad.
SecAddSites desactiva la posibilidad de añadir *Sitios* web a las diferentes zonas de seguridad.
ContentTab desactiva la pestaña *Contenido*.
FormSuggest desactiva *Auto Completar* para los formularios.
FormSuggest Passwords desactiva el cuadro de diálogo *Preguntar si se guardan las contraseñas*.
Wallet (sólo en Internet Explorer 4.0) desactiva la billetera virtual que almacena la configuración de nuestras tarjetas de crédito.
Profiles desactiva la configuración del *Asistente de perfiles* .
Ratings desactiva el *asesor de contenido*.
ConnectionsTab desativa la pestaña *Conexiones*.
Proxy desactiva la configuración del *proxy*.
Connection Settings desactiva la configuración de las conexiones de acceso telefónico y redes privadas.
Connection Wizard desactiva el asistente para nuevas conexiones.
ProgramsTab desactiva la pestaña *Programas*.
ResetWebSettings desactiva el botón *Restablecer configuración web* de los programas externos a Internet Explorer.
Messaging desactiva la configuración del programa de *correo electrónico*.
Calendar desactiva la configuración del programa de *Calendario*.
Contact desactiva la configuración del programa de *Lista de contactos*.
Check_If_Default desactiva la casilla *Comprobar si Internet Explorer es el explorador predeterminado*.
AdvancedTab o *Advanced* desactiva la pestaña *Opciones Avanzadas*.
Conviene tener en cuenta que algunas claves no existen en todas las versiones de Internet Explorer. Estas restricciones pueden ser utilizadas para un usuario concreto añadiendo las modificaciones a la clave *HKEY_CURRENT_USER* o a una máquina en general añadiéndolas bajo la clave *HKEY_LOCAL_MACHINE*. Además, será necesario reiniciar Windows para que los cambios surtan efecto.



Outlook Express 6.0

Aprovecha al máximo la última versión de este programa

Outlook Express 6.0 es la evolución del críptico *Internet Mail and News* que apareciera con la versión 3.0 de la *suite* Internet Explorer. Desde entonces, con cada nueva revisión se han añadido más funcionalidades hasta convertirlo en el cliente de correo gratuito más utilizado en el mundo. Y es que el correo electrónico es una herramienta que pone al alcance de toda la gente, independientemente de su localización, clase social o conocimientos de informática, la comunicación.



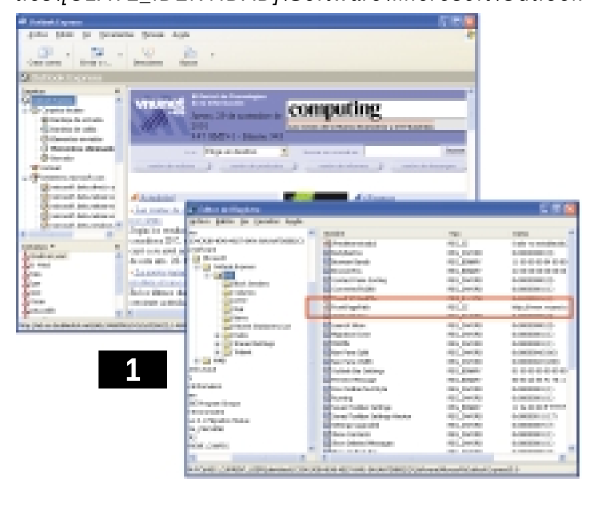
El mundo empresarial, científico, universitario, doméstico, etc., no pueden entenderse ya sin las posibilidades que la mensajería electrónica ofrece. Por ello, Outlook Express integra en un mismo cliente la posibilidad de gestionar múltiples cuentas de correo electrónico POP3, IMAP y HTTP, y cuentas de servidores de noticias y mensajería instantánea gracias a su integración con Windows Messenger. En esta última versión 6.0 se han potenciado las características de seguridad, ya que hoy en día el correo electrónico es una puerta de entrada a multitud de virus, gusanos y troyanos de todo tipo. Las siguientes páginas os ayudarán a sacar el máximo provecho a todas las facetas que encierra Outlook Express 6.0.

General y vistas

1 Cambiar la página de inicio de Outlook Express

Intermedio

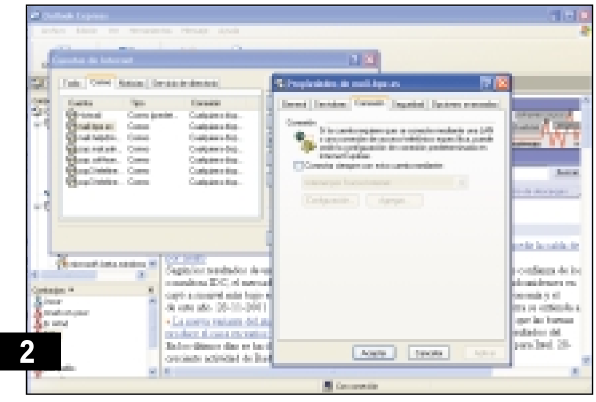
La página que Outlook Express carga en la parte derecha de la ventana principal cuando iniciamos el programa puede ser modificada mediante la edición del registro. Para ello iniciaremos la herramienta «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Identities\[CLAVE_IDENTIDAD]\Software\Microsoft\Outlook Express\5.0*. Allí modificaremos el contenido del valor de tipo alfanumérico FrontPagePath indicando la página local o dirección URL que utilizaremos como página de bienvenida. Cerraremos el registro y reiniciaremos Outlook Express para que los cambios surtan efecto.


1

2 Automatizar el proceso de conexión

Intermedio

Muchos usuarios utilizan Internet solamente para acceder a su correo electrónico, y algunos de ellos desearían que Outlook Express fuera capaz de conectarse, comprobar y descargar los mensajes y desconectarse automáticamente. Esto es posible, siempre y cuando dejemos Outlook Express abierto, por ejemplo, en modo minimizado. En primer lugar,

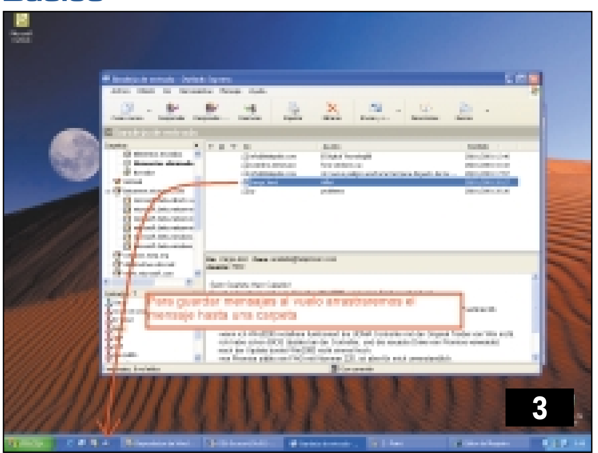

2

dentro del menú *Herramientas/Opciones/General* estableceremos el valor apropiado en la casilla *Comprobar nuevos mensajes cada "x" minutos*. Acto seguido comprobaremos que todas nuestras cuentas (de correo y de noticias) estén configuradas, dentro del menú *Herramientas/Cuentas/Correo (o) Noticias/[Nombre_de_cuenta]/Propiedades/Conexión* para utilizar la misma conexión de acceso telefónico a redes y asegurándonos de que en la configuración del acceso telefónico a redes la casilla *Recordar contraseña* esté marcada y con la contraseña correcta introducida para cada una de las cuentas. Bajo el mismo menú *Herramientas/Opciones*, en la pestaña *General* seleccionaremos de la lista desplegable la opción *Conectar sólo cuando no trabaje sin conexión* y en la pestaña *Conexión* marcaremos la casilla *Colgar después de enviar y recibir*.

Cliente de correo electrónico y lector de noticias

3 Guardar mensajes y datos adjuntos al vuelo

Básico

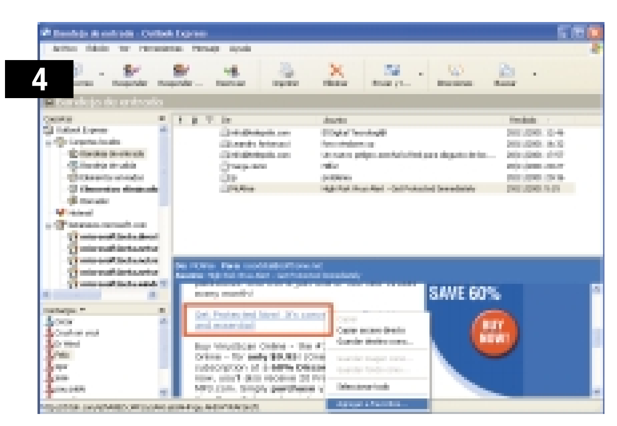


Si tenemos una gran cantidad de archivos adjuntos en nuestros correos electrónicos que queremos guardar en nuestro sistema, podemos utilizar la opción *Guardar como* y buscar hasta encontrar la unidad de disquete o el directorio donde queremos almacenar el archivo. Sin embargo, existe un método más rápido consistente en crear un acceso directo en el menú de *Inicio rápido* de la *Barra de tareas*, al directorio o unidad donde normalmente guardemos los archivos adjuntos. De este modo, cuando queramos salvar algún archivo adjunto en ese directorio, todo lo que tendremos que hacer será arrastrarlo desde el correo electrónico. Este método puede ser utilizado además para guardar mensajes de correo electrónico o de envíos a foros de noticias, en cuyo caso serán salvados como archivos «*.eml» o «*.nws», respectivamente.

4 Añadir direcciones URL a los favoritos desde Outlook Express

Básico

Añadir una dirección URL a los favoritos almacenados en Internet Explorer desde Outlook Express es tan sencillo como hacer clic con el botón derecho del ratón sobre el hiperenlace que encontraremos en el cuerpo del mensaje y seleccionar en el menú contextual la opción *Añadir a favoritos*. Sin embargo,

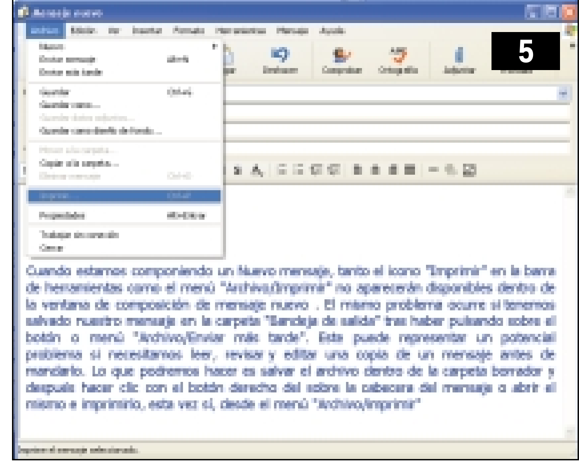


este enlace será creado en la carpeta principal de *Favoritos*, por lo que tendremos que definir mejor su ubicación desde Internet Explorer en caso necesario.

5 Imprimir mensajes que no han sido enviados

Básico

Cuando estamos componiendo un nuevo mensaje, tanto el icono *Imprimir* en la *Barra de herramientas* como el menú *Archivo/Imprimir* no aparecerán disponibles dentro de la ventana de composición de mensaje nuevo. El mismo problema ocurre si tenemos salvado nuestro mensaje en la carpeta *Bandeja de sali-*

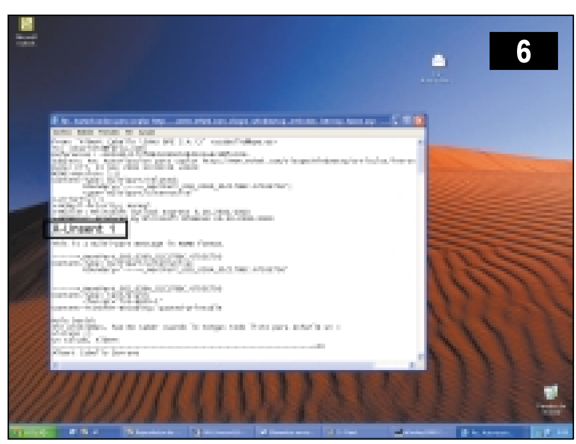


da tras haber pulsado sobre el botón o menú *Archivo/Enviar más tarde*. Esto puede representar un problema si necesitamos leer, revisar y editar una copia de un mensaje antes de mandarlo. Lo que podremos hacer es salvar el archivo dentro de la carpeta *Borrador* y después hacer clic con el botón derecho del ratón sobre la cabecera del mensaje o abrir el mismo e imprimirlo, esta vez sí, desde el menú *Archivo/Imprimir*.

6 Cómo volver a enviar un mensaje

Intermedio

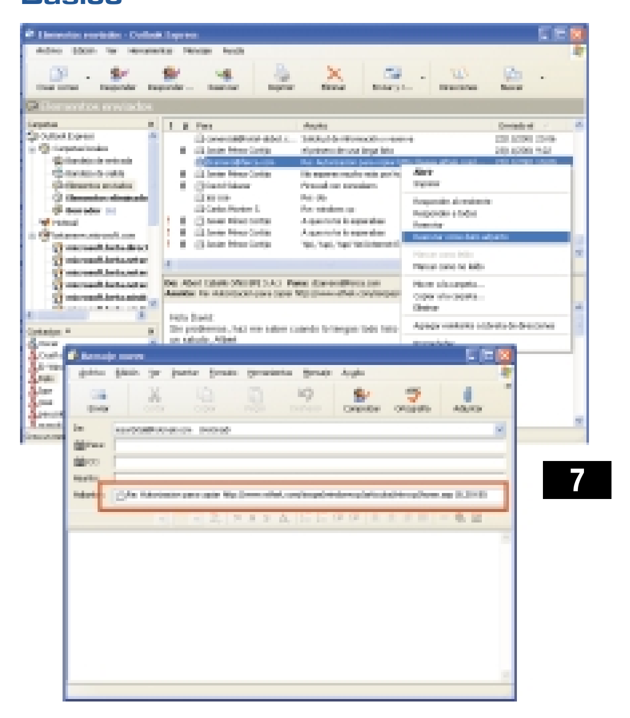
Desafortunadamente, Outlook Express no tiene implementada una función de volver a enviar una copia exacta de un mensaje ya enviado. En su lugar, podemos suplir esta carencia abriendo la copia original del archivo enviado, que encontraremos dentro de la carpeta *Elementos enviados*. Dentro del menú *Archivo* seleccionaremos la opción *Guardar como* y salvaremos el mensaje en nuestro escritorio como un archivo de tipo «.eml». Abriremos este archivo con el bloc de notas



(«notepad.exe») y añadiremos la línea *X-Unsent: 1* a las cabeceras existentes, junto con el resto de líneas que comienzan con los caracteres *X-*. Salvaremos el archivo editado, haremos doble clic sobre el mismo y podremos enviarlo pulsando el botón *Enviar*.

7 Reenviar la información de la cabecera de un mensaje

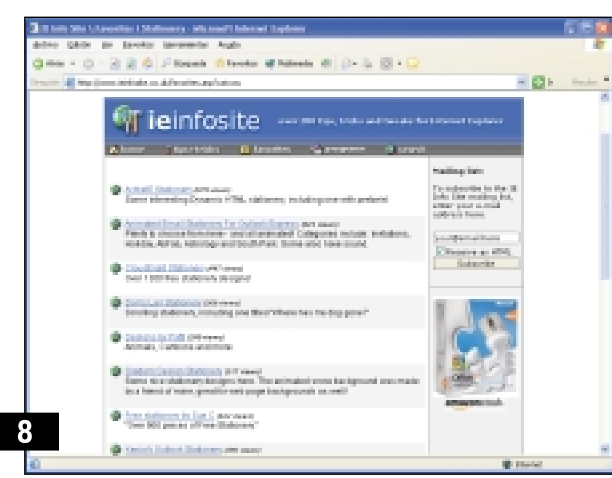
Básico



Muchos usuarios necesitan una manera de aislar y enviar la información detallada de la cabecera de un mensaje en particular a otro usuario a través del correo electrónico. La manera más fácil de hacerlo es simplemente utilizando la opción del menú contextual *Reenviar como archivo adjunto*. Esta opción de menú fue añadida a Outlook Express específicamente para poder enviar mensajes con la información de la cabecera original intacta. Otro método que también funciona, pero no es fácil de llevar a cabo es seleccionar la cabecera del mensaje y pulsar «Ctrl+F3». Cuando aparezca la ventana de código fuente del mensaje, copiaremos los detalles de la cabecera que necesitemos archivando esa información en una copia reenviada del mensaje del que hemos aislado su cabecera.

8 Diseños de fondo para Outlook Express

Básico

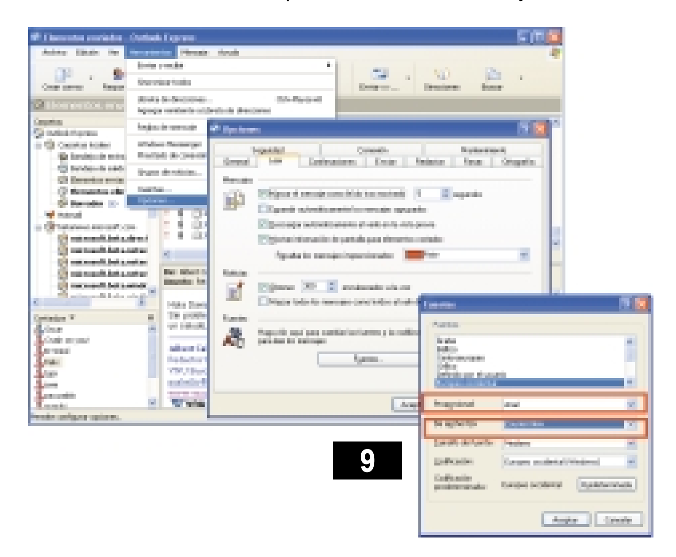


Los diseños de fondo son pequeñas plantillas HTML que podemos añadir a nuestro mensajes para darle un toque de elegancia a nuestras comunicaciones. En la página *www.ieinfosite.co.uk/favorites.asp?cat=os* encontraremos enlaces a varias páginas con miles de diseños de fondo para nuestro correo.

9 Cómo ver mensajes con un tamaño y tipo de fuente fijos

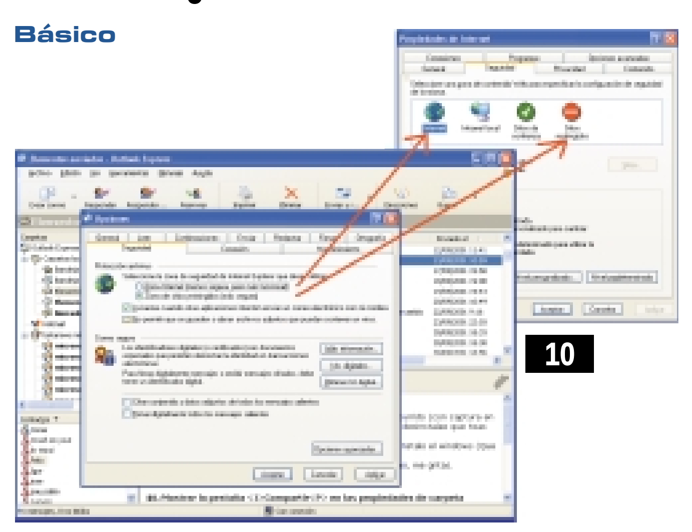
Básico

Los mensajes que utilizan HTML en su composición contienen tamaños y tipos de fuente que a muchos usuarios les puede resultar difícil su lectura. Para leer un mensaje concreto con un tipo y tamaño de fuente fijos, seleccionaremos, una vez nos encontremos en la ventana de mensaje, el menú *Ver/Tamaño de texto/Fijo*. Esta fuente fija será únicamente utilizada para este mensaje concreto, y su utilización será olvidada cuando cerremos el mismo. Para ver todos los mensajes haciendo uso de una fuente y tamaño fijos, acudiremos al menú *Herramientas/Opciones/Leer/Fuentes* y en la lista de *Fuente proporcional* seleccionaremos un tipo de fuente «de ancho fijo».



10 Cómo monitorizar los contenidos descargados

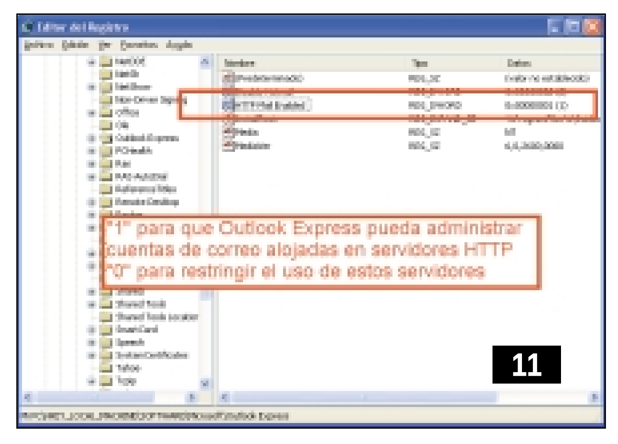
Básico



Utilizar HTML en los grupos de noticias o en los mensajes de correo electrónico siempre es un motivo de disputa en el que no todos estamos de acuerdo. Sin embargo, como primera capa de seguridad y para aumentar la velocidad en la descarga de mensajes que utilicen este formato, Outlook Express respeta la configuración con respecto a contenidos como sonidos, gráficos, etc., que se establece dentro de la configuración de Internet Explorer, y que encontraremos en el menú *Herramientas/Opciones de Internet* bajo la pestaña *Avanzada*. Allí podremos ajustar y desactivar los elementos que deseemos.

11 Controlar el uso de correo electrónico HTTP

Intermedio



Mediante la edición del registro podemos definir si Outlook Express podrá administrar cuentas de correo ubicadas en servidores HTTP, como es el caso de las cuentas de Hotmail. Para ello iniciaremos la herramienta de edición del registro de sistema, con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Outlook Express*. Allí crearemos o modificaremos el valor DWORD existente HTTP Mail Enabled cuyo contenido será 0 para deshabilitar el uso de este tipo de cuentas o 1 para continuar haciendo uso de ellas.

12 Outlook Express y las cuentas de correo IMAP

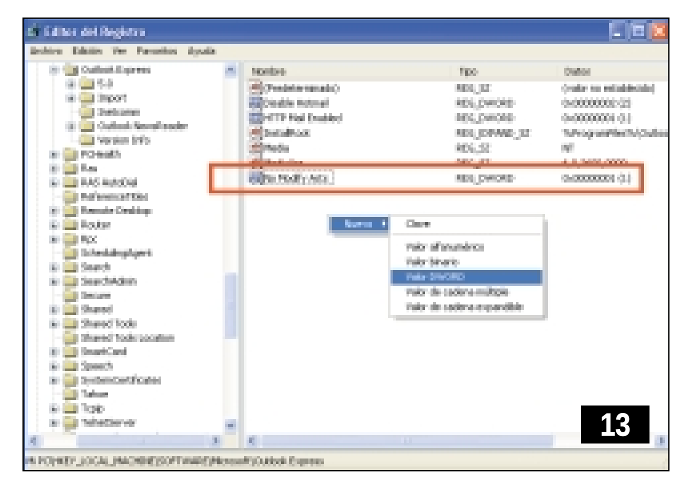
Intermedio

Mediante la edición del registro podemos controlar el comportamiento de Outlook Express con las cuentas de correo IMAP, para que utilice las carpetas *Borrador* y *Elementos enviados* del servidor IMAP en vez de duplicar los contenidos en las carpetas locales. Para ello iniciaremos el editor de registro del sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\{Identificador_de_cuenta}*, donde el «Identificador de cuenta» será el número relacionado con la cuenta IMAP, por ejemplo 00000002. En caso necesario nuestro administrador de sistema encontrará y nos proporcionará el nombre de las carpetas de nuestra cuenta IMAP: *Bandeja de entrada* (normalmente. *Inbox*), la carpeta *Borrador* (*Drafts*) y la carpeta de *Elementos enviados* (*Sent-Mail*). Crearemos nuevos valores de tipo alfanumérico o modificaremos los ya existentes IMAP Root folder, IMAP Drafts folder e IMAP Sent items folder, estableciendo su contenido de acuerdo con los resultados obtenidos en el paso anterior. Cerraremos el registro y reiniciaremos Outlook Express para que los cambios surtan efecto.

13 Cómo evitar alteraciones en la configuración de cuentas

Intermedio

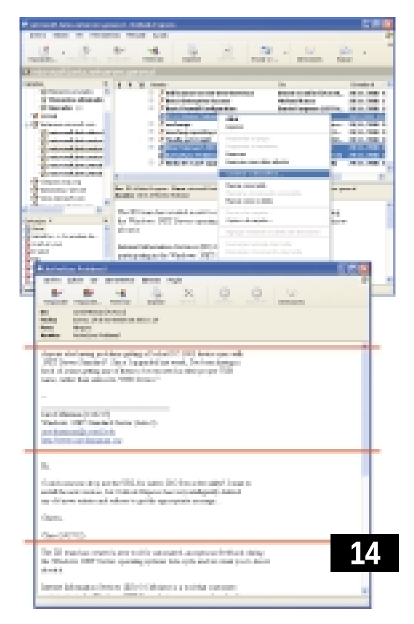
Si editamos el registro de sistema podemos configurar Outlook Express para que permita o evite que los usuarios creen o modifiquen la configuración de cualquier cuenta de correo, noticias o directorios. Para ello iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\-Outlook Express*. Allí crearemos un valor DWORD o modificaremos el existente No Modify Acts cuyo contenido será 1 para activar la restricción o 0 para permitir que los usuarios modifiquen la configuración de las cuentas. Tendremos que reiniciar Outlook Express para que los cambios se lleven a cabo.



14 Imprimir y guardar múltiples mensajes de noticias como un único mensaje

Básico

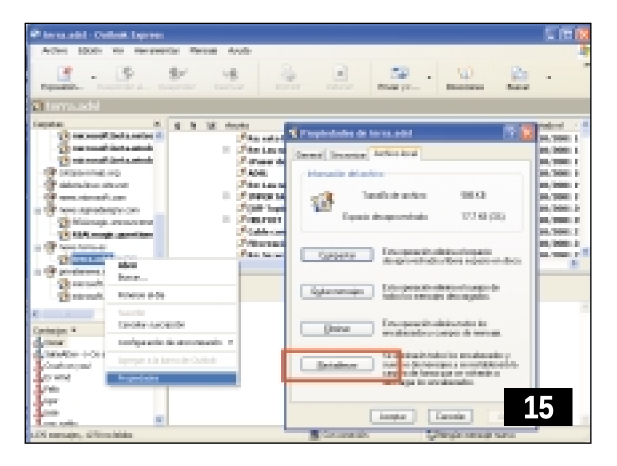
Otra utilidad de la función *Combinar y decodificar* de Outlook Express, exceptuando su uso en los grupos binarios, es la posibilidad de combinar el contenido de texto de múltiples mensajes de un grupo de noticias, de forma que podamos imprimirlos o leerlos más tarde como sin fueran un único mensaje, algo que puede resultar útil en aquellos hilos de conversación con gran cantidad de respuestas. Para ello nos conectaremos a nuestro servidor de noticias, seleccionaremos uno a uno los mensajes en el grupo de noticias cuyo contenido queremos combinar y utilizaremos en el menú contextual, que aparece al pulsar el botón derecho del ratón, la opción *Combinar y decodificar*. Tras verificar el correcto orden de los mensajes, éstos serán combinados en un único mensaje, el cual deberemos guardar en alguna carpeta de Outlook o como archivo «.eml» en el disco duro o imprimir su contenido, ya que si no lo hacemos, el mensaje combinado no quedará salvado en sitio alguno, y tendremos que volver a combinarlo de nuevo.



15 Cómo restablecer la lista de mensajes de un grupo de noticias

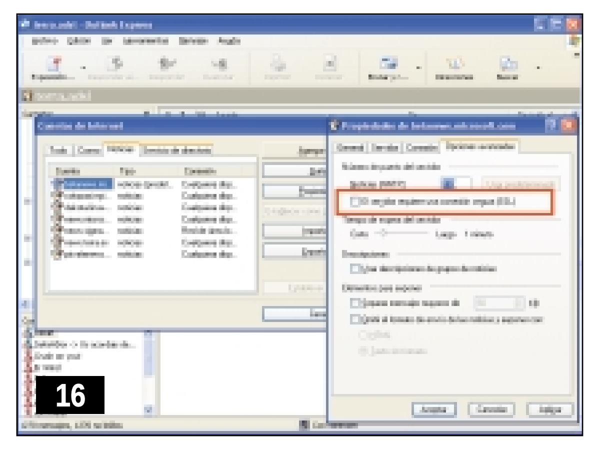
Básico

Existen multitud de razones para querer restablecer la lista de mensajes de un grupo de noticias. Una de ellas puede ser la sospecha de que nuestro archivo «.nch», encargado de listar los mensajes del grupo y de diferenciar entre los leídos, no leídos, descargados… se haya corrompido, algo que notaremos cuando Outlook Express no mantenga nuestras marcas de seguimiento a hilos determinados, o todas las cabeceras de los grupos de noticias hayan sido marcadas como leídos, etc. Outook Express dispone de una manera fácil de manejarse con estos problemas. Seleccionaremos un grupo de noticias en la lista de carpetas, haciendo clic con el botón derecho del ratón sobre el mismo. Después seleccionaremos sus *Propiedades* y nos iremos hasta la pestaña *Archivo local*. Una vez allí, buscaremos el botón *Restablecer*. Pulsando sobre esta opción, Outlook Express purgará toda la información previamente almacenada por el programa sobre este grupo de noticias, incluyendo la caché de mensajes leídos. Esto significa que la próxima vez que visitemos el grupo de noticias, todos los mensajes serán descargados y recreados, y todos ellos marcados como no leídos.



16 Añadir servidores seguros

Básico

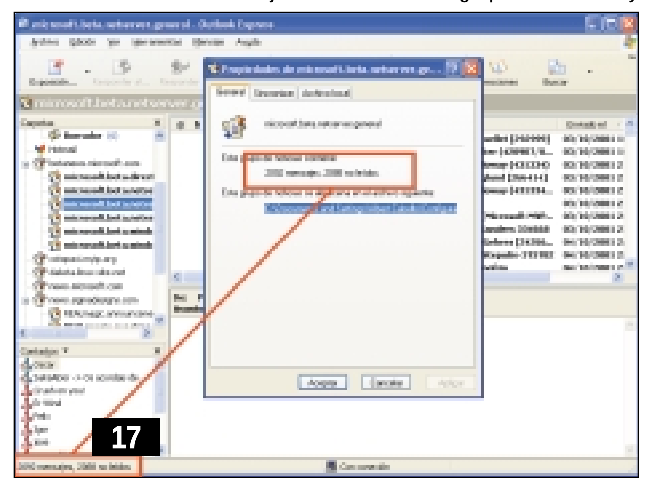


Para añadir un servidor que requiera una conexión segura (como SSL), lo haremos igual que con un servidor normal, seleccionando el menú *Herramientas/Cuentas/Añadir/Noticias*. Sin embargo, una vez creada la conexión, nos desplazaremos hasta sus *Propiedades* y haremos clic sobre la pestaña *Opciones Avanzadas*. Allí marcaremos la casilla *Este servidor requiere una conexión segura (SSL)*. Dejando activada esta opción, automáticamente se cambiará el número del puerto al utilizado para las conexiones seguras con los servidores.

17 Mensajes en un grupo de noticias

Básico

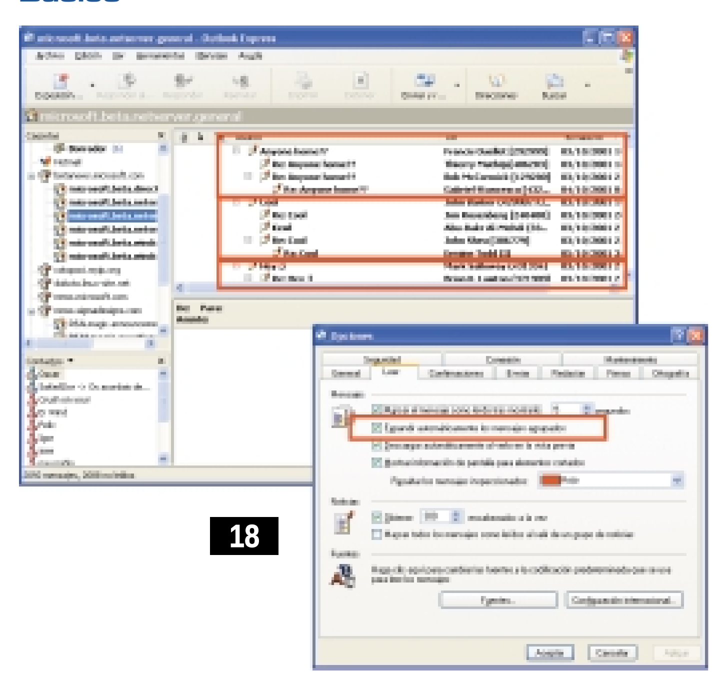
A medida que los mensajes de un grupo de noticias no sean marcados como leídos, Outlook Express comenzará a informar incorrectamente junto al nombre del grupo de noticias y



entre paréntesis los mensajes sin leer contenidos en una carpeta. Sin embargo, cada cierto tiempo podemos necesitar saber el número de mensajes totales existentes (por ejemplo, leídos y no leídos) en una carpeta determinada. Para ello tenemos dos métodos: el primero es hacer clic con el botón derecho del ratón sobre el nombre de un grupo de noticias y seleccionar en el menú contextual sus *Propiedades*. El cuadro de diálogo resultante nos informará del número de mensajes en el grupo y los que no han sido leídos. El segundo de los métodos es entrar dentro de un grupo de noticias y comprobar el número que aparecerá en la parte inferior izquierda dentro de la barra de estado.

18 No perder el hilo

Básico

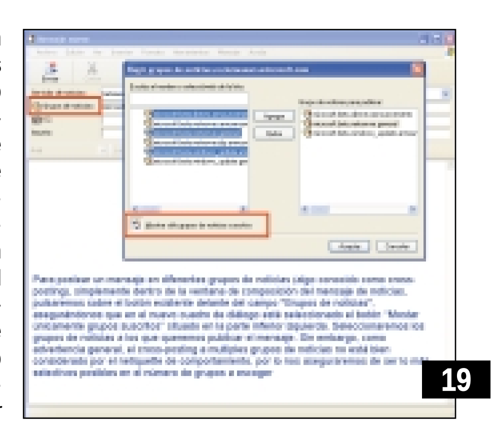


Si queremos que Outlook Express muestre automáticamente todos los hilos de los grupos de noticias extendidos, simplemente marcaremos dentro del menú *Herramientas/Opciones,* bajo la pestaña *Leer*, la opción *Expandir automáticamente los mensajes agrupados*.

19 *Cross-posting* de mensajes

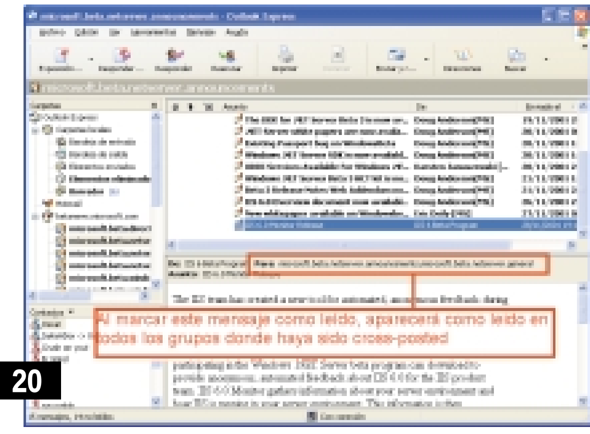
Básico

Para publicar o enviar un mensaje en diferentes grupos de noticias (algo conocido como *cross-posting*), simplemente dentro de la ventana de composición del mensaje de noticias pulsaremos sobre el botón existente delante del campo *Grupos de noticias*, asegurándonos de que en el nuevo cuadro de diálogo esté seleccionado el botón *Mostar sólo grupos de noticias suscritos*, situado en la parte inferior izquierda. Seleccionaremos los grupos de noticias en los que queremos publicar el mensaje. Como advertencia general, el *cross-posting* a múltiples grupos de noticias no está bien considerado, por lo que nos aseguraremos de ser lo más selectivo posible en el número de grupos a escoger.



20 Efecto de marcar como leído un mensaje *cross-posted*

Básico

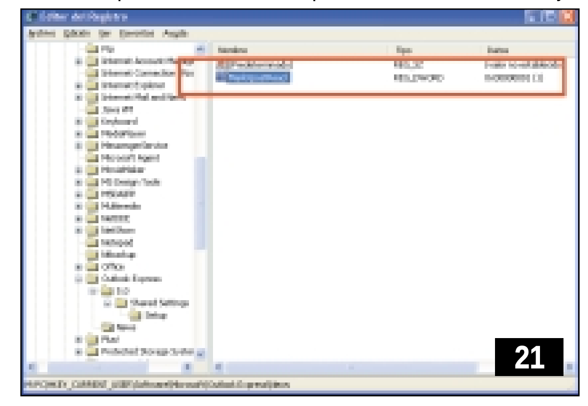


Al abrir en un grupo de noticias, un mensaje que ha sido publicado en varios de los grupos del servidor (*cross-posted*) será marcado como leído en el resto de grupos de noticias donde haya sido publicado. Como resultado, si el mensaje ha sido publicado en un segundo grupo de noticias al que estamos suscrito, haremos uso de la opción *Mensajes no leídos* situada bajo el menú *Ver/Vista actual*, de forma que, cuando abramos el segundo grupo de noticias, el mensaje marcado como leído en el primer grupo no aparecerá de nuevo como tal.

21 Manejar independientemente mensajes *cross-posted*

Avanzado

Como hemos indicado en el anterior truco, al marcar los mensajes como leídos, Outlook Express trata como un mismo mensajes todas las copias *cross-posted*. Sin embargo, podemos modificar este comportamiento a nuestra elección. Una razón para hacerlo es que mientras leamos un mensaje en un grupo podemos no darnos cuenta de la existencia de una respuesta que solucione nuestro problema en otro de los grupos en los que hayamos publicado el mensaje. Si queremos que Outlook Express administre independientemente los mensajes



cross-posted, iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\News*. Allí crearemos o modificaremos el valor DWORD existente (MarkXpostRead), cuyo contenido será 0 para administrar de forma separada cada una de las copias *cross-posted* del mensaje o 1 para tratarlos como un único mensaje.

22 Cancelar un mensaje *cross-posted*

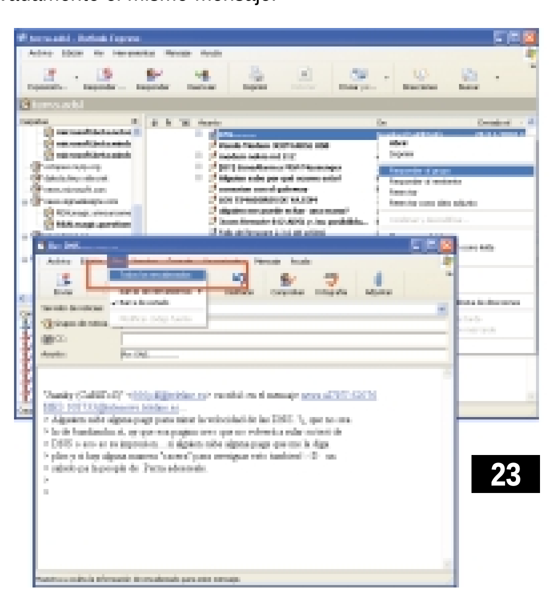
Intermedio

Dependiendo de la configuración que haga el administrador, Outlook Express nos brindará la posibilidad de cancelar o eliminar un mensaje que ya esté publicado en un foro de noticias creado por nosotros. Para ello pulsaremos con el botón derecho del ratón sobre su cabecera y en el menú contextual seleccionaremos la opción *Cancelar*. Hasta el momento en que se procese la orden de cancelación, el programa nos mostrará un mensaje de confirmación del servidor de noticias que dirá: «Su petición de cancelación ha sido enviada al servidor de noticias. El mensaje cancelado puede no desaparecer de inmediato». Si no aparece esta opción, será debido a que el administrador tiene esta función desactivada.

23 Que nadie se quede sin su respuesta

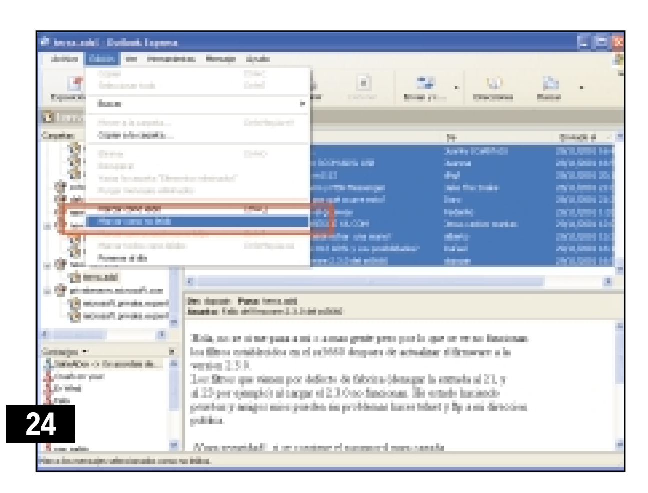
Básico

Muchos usuarios preguntan cómo enviar una repuesta tanto a un mensaje publicado en un servidor de noticias como privadamente a la dirección de correo electrónico del remitente. La respuesta está en seleccionar en el menú contextual o en la barra de botones de la ventana del mensaje la opción *Responder al grupo*, tras lo cual haremos lo mismo en el menú *Ver* la opción *Todos los encabezados*. De esta manera aparecerá un nuevo cuadro en el que podremos introducir la dirección de correo electrónico de cuantas personas queramos mandar privadamente el mismo mensaje.



24 No marcar todos los mensajes como leídos

Básico

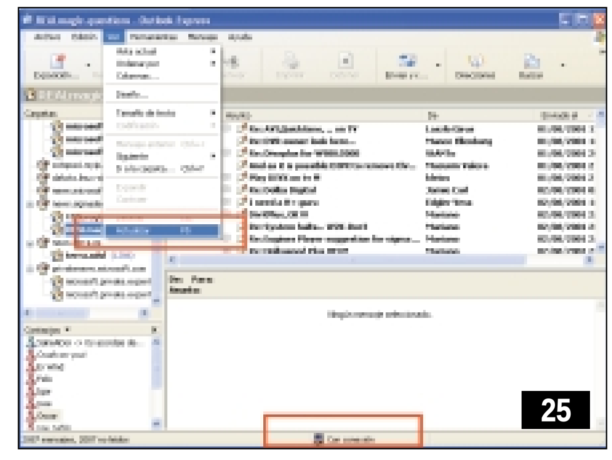


Si por equivocación hemos utilizado mientras visitábamos un grupo de noticias la opción *Marcar todos como leídos* dentro del menú *Edición* o el botón *Marcar todos como leídos*, si hemos personalizado nuestra barra de herramientas todavía podemos deshacer esta acción. En primer lugar seleccionaremos en el menú *Editar* la opción *Seleccionar todo* y después dentro del mismo menú *Marcar como no leído*. Aunque este método no es muy intuitivo, funciona.

25 Reconectar al servidor

Básico

Un problema común en los foros de noticias es que mientras estamos componiendo un mensaje de gran tamaño podemos ser desconectados del servidor de noticias. Al contrario que otros gestores de noticias, el incluido en el Outlook Express incorpora una ventana de notificación que nos informará cuando la conexión con el servidor de noticias haya finalizado. En ese caso tendremos un par de opciones para reconectarnos al servidor, asumiendo que todavía estamos conectados con nuestro proveedor de Internet. La primera de ellas, haciendo doble clic sobre el icono *Trabajando on-line* que encontraremos en la barra de estado de la ventana principal. La segunda es a través del menú *Ver* y seleccionando la opción *Refrescar* o con el método abreviado de teclado «F5», que forzará un intento de reconexión con el servidor.



26 La lentitud de Outlook Express al trabajar con cuentas de noticias

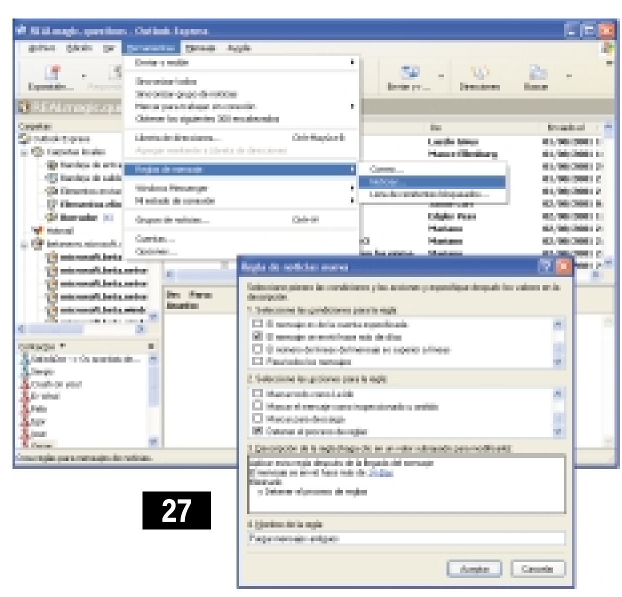
Básico

La causa habitual que provoca el lento funcionamiento repentino de Outlook Express al trabajar con los grupos de noticias, suele ser el gran tamaño de los archivos que se generan al visitar grupos con gran cantidad de encabezados, aunque éstos estén marcados como ya leídos y ocultos aplicando las diferentes vistas. Cuando notemos que un grupo de noticias se vuelve lento, es momento para limpiar nuestros grupos y compactar nuestras carpetas. Si el rendimiento es lento cuando abrimos por primera vez un grupo de noticias o al intercambiar entre grupos de noticias diferentes, esto puede ser debido a que nuestra cuenta de noticias soporte un gran número de grupos de noticias. Rara vez nos ocurrirá esto en sistemas con grandes cantidades de memoria o en cuentas con menos de 25.000 grupos de noticias.

Reglas

27 Usar reglas para eliminar viejos mensajes en grupos de noticias

Avanzado

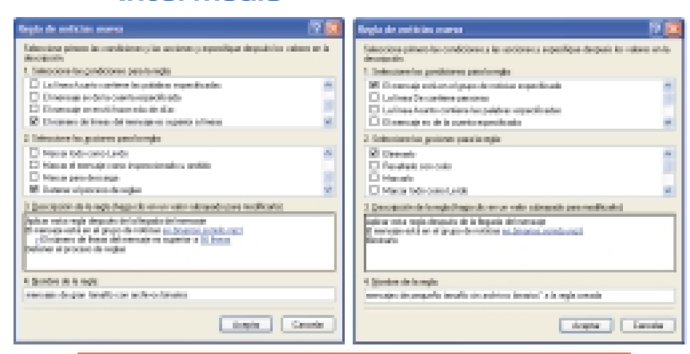


27

Outlook Express no incluye ninguna opción para eliminar las cabeceras de viejos mensajes de noticias, a excepción de aquellos cuyo cuerpo del mensaje también haya sido descargado, en cuyo caso se aplicará la configuración establecida en el menú *Herramientas/Opciones* de Outlook Express, situada bajo la pestaña *Mantenimiento*. Sin embargo, podemos utilizar las reglas de mensaje para realizar esta tarea. Bajo el menú *Herramientas/Reglas de mensaje/Noticias* crearemos la siguiente regla:
El mensaje se envió hace más de "días"
Eliminarlo
Detener el proceso de reglas
Estableceremos como valor del campo "días" 14 (2 semanas), y definiremos la regla como «Purgar mensajes antiguos». Ahora desmarcaremos la casilla delante de la regla para desactivarla, ya que de esta manera Outlook Express aplicaría la regla automáticamente y podría eliminar mensajes que todavía necesitamos. Hay que recordar que las reglas serán aplicadas automáticamente cuando un mensaje o cabecera sea descargado por primera vez, y lo que nosotros queremos es crear una regla para los mensajes y cabeceras que ya hayan sido descargados. Cuando queramos eliminar las viejas cabeceras, pulsaremos sobre el menú *Herramientas/Reglas de mensaje/Noticias* y marcaremos la casilla *Aplicar ahora*. Para aplicar la regla a todos los grupos en una cuenta de noticias nos desplazaremos hasta el icono de la propia cuenta. Y para aplicar la regla a todos los grupos en todas las cuentas de noticias, nos desplazaremos hasta el icono Outlook Express. Por supuesto, podremos usar otras condiciones en nuestra regla o crear varias reglas según las necesidades. Tras finalizar la regla, cerraremos el cuadro de diálogo *Reglas de mensaje* y compactaremos las carpetas cuyo contenido hayamos purgado.

28 Reglas y grupos de noticias binarios

Intermedio



28 Para eliminar archivos "no binarios" en grupos de noticias binarios, tendremos que crear dos reglas que diferenciarán los dos tipos de mensajes por su número de líneas

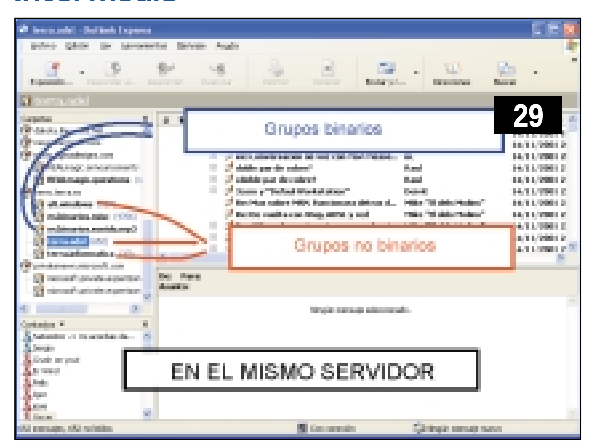
Muchos usuarios encontrarán útil el uso de reglas de mensaje para evitar en los grupos de noticias la descarga de mensajes de gran tamaño. Sin embargo, para los usuarios que frecuentemente visiten grupos de noticias binarios, en los que los mensajes publicados contienen gran cantidad imágenes, sonidos, películas y archivos adjuntos, puede ser de gran ayuda el hecho de agilizar la descarga evitando todo lo contrario: descargar los mensajes más pequeños. Esto se debe a que, en estos grupos de noticias, un mensaje de pequeño tamaño es normalmente un *spam* o una petición de reenvío de otro mensaje, mientras que un mensaje de gran tamaño suele contener un archivo adjunto binario en su contenido. Como las reglas de mensaje de Outlook Express únicamente nos permiten filtrar mensajes con un número *mayor* y no *menor*, aparentemente no resulta obvio cómo proceder. La respuesta está en crear dos reglas en vez de una.
La primera:
Cuando el mensaje está en el grupo de noticias "especificado"
El número de líneas del mensaje es superior a "líneas"
Detener el proceso de reglas
Estableceremos como grupo de noticias "especificado" el nombre del grupo o servidor de noticias que tenga archivos binarios y como número de "líneas" 50, y definiremos la regla como «mensajes de gran tamaño con archivos binarios».
Ahora crearemos la segunda regla:
Cuando el mensaje está en el grupo de noticias "especificado"
Eliminarlo
Detener el proceso de reglas
Estableceremos como grupo de noticias "especificado" el mismo que definimos en la anterior regla, y le daremos el nom-

bre «mensajes de pequeño tamaño sin archivos binarios» a la regla creada.

La primera regla evitará procesar ninguna regla más para cualquier mensaje cuyo cuerpo contenga más de 50 líneas. La segunda regla eliminará todos los mensajes que no cumplan la primera regla, refiriéndose a aquellos con menos de 50 líneas. El grupo de noticias resultante tendrá únicamente mensajes con más de 50 líneas. Es necesario destacar que, si queremos aplicar otras reglas para los mensajes de gran tamaño, tendremos que situarlos en la lista de reglas por encima de la regla de archivos binarios de gran tamaño, ya que de lo contrario no serán procesadas.

29 Reglas y servidores de noticias con grupos binarios y no binarios

Intermedio

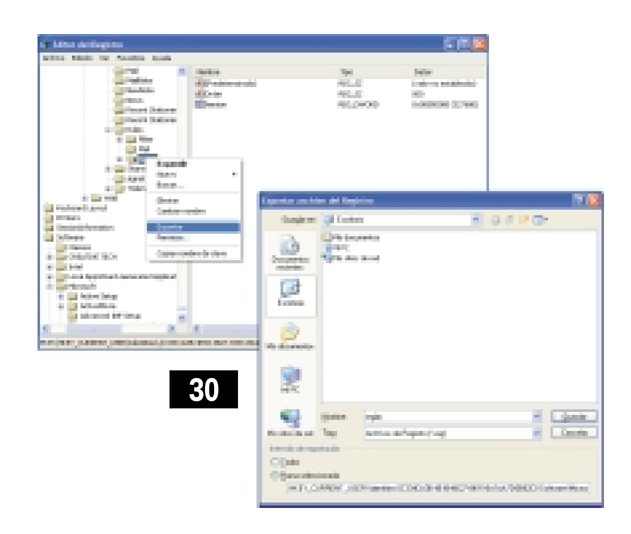


Si nos suscribimos a varios grupos binarios y varios grupos no binarios y utilizamos reglas para filtrar los mensajes o su contenido, será preferible utilizar diferentes cuentas de noticias, de acuerdo con los tipos de los grupos, aunque ambas utilicen el mismo servidor de noticias. En otras palabras, deberemos suscribirnos a todos los grupos binarios en la cuenta de noticias «Número 1» y a todos los grupos no binarios en la cuenta de noticias «Número 2», aunque ambas cuentas utilicen el mismo servidor. Esto nos permitirá utilizar reglas de mensajes para una cuenta entera en vez de un grupo de noticias específico. Suscribirse a grupos de noticias binarios en una cuenta de binarios no requerirá configuración posterior alguna además de las reglas ya aplicadas al servidor completo. Si no queremos utilizar cuentas separadas para los grupos binarios, tendremos que duplicar ambas reglas para cada grupo de noticias de archivos binarios a los que nos suscribamos, ya que de lo contrario también afectarían a los grupos de noticias no binarios. Si optamos por múltiples cuentas de grupos de noticias utilizando el mismo servidor de noticias, haremos bien en mantener todas excepto una cuenta libre con la lista completa de los grupos de noticias. Esto conlleva algo de trabajo a la hora de la configuración, pero incrementará el rendimiento, algo que a buen seguro nos valdrá la pena.

30 Copia de seguridad de las reglas

Intermedio

Después de emplear una considerable cantidad de tiempo creando y perfilando las reglas para filtrar nuestro correo entrante y la suscripción a grupos de noticias, muchos usuarios preferirían no tener que volver a recrearlos jamás, de modo que necesitamos una forma que nos permita reinstalarlos en otro ordenador o en el



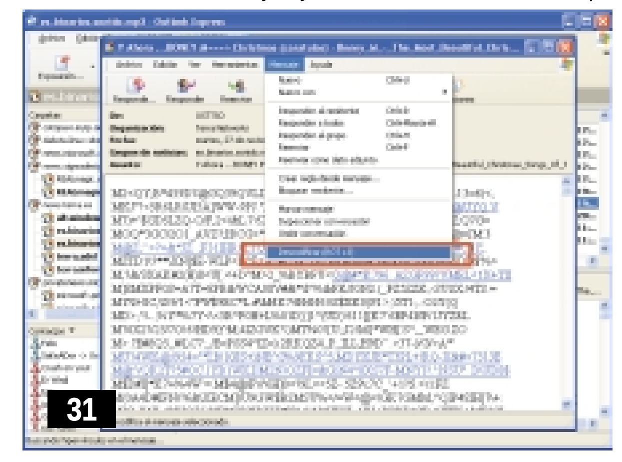
mismo después de un formateo y una reinstalación del sistema. Para realizar esta copia de seguridad, simplemente iniciaremos la herramienta de edición del registro con el comando «regedit.exe» desde el menú *Inicio/Ejectuar*. Allí localizaremos la clave *HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\5.0\News\Group Filters* o *HKEY_CURRENT_USER\Identities\[Clave_identidad]\Software\Microsoft\Outlook Express\5.0\Rules\News* dependiendo de si utilizamos Outlook Express 5.x o 6.0, y dentro del menú *Registro/Exportar archivo de registro* realizaremos la exportación a un archivo que llamaremos «reglas.reg» y que guardaremos en lugar seguro.

Seguridad y solución de problemas

31 El sistema de descifrado ROT 13

Básico

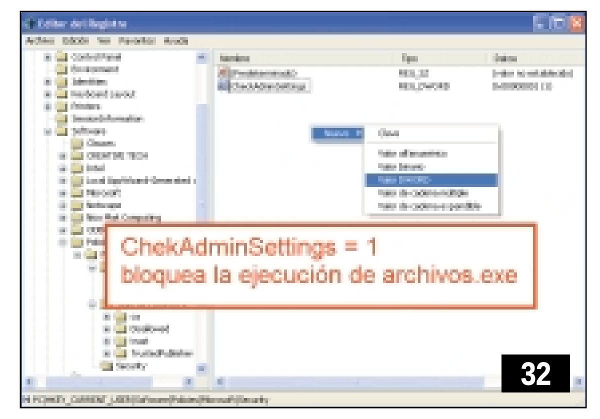
En ocasiones puede ocurrirnos que un mensaje en un foro de noticias aparezca cifrado. Outlook Express ofrece soporte para un sencillo método de cifrado de correo, llamado ROT 13. Para leer un mensaje cifrado en ROT 13, dentro de la ventana mensaje seleccionaremos en el menú *Edición* la opción *Descodificar (ROT 13)*. Sin embargo, nos preguntaremos por qué la gente utiliza ROT 13 sin descifrar su contenido. ROT 13 se utiliza principalmente para advertir a la gente de que el mensaje puede contener material que resulte ofensivo. De esta forma, el lector queda advertido y tiene la opción de no descifrar el mensaje. Normalmente podemos hacernos una idea de la naturaleza del mensaje leyendo la información en el campo



Asunto. Esto nos ayudará a decidir si descifrar un mensaje. Adicionalmente, ROT 13 evita el envío en modo texto plano de los mensajes entre nosotros y el servidor, de forma que es más difícil que sea interceptado por usuarios maliciosos.

32 Cómo controlar las características de seguridad

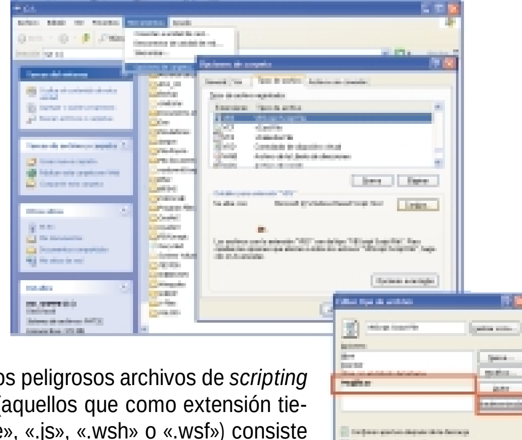
Avanzado



Outlook Express incluye una característica de seguridad que permite desactivar la posibilidad de abrir directamente archivos ejecutables («.exe»). Sin embargo, se encuentra deshabilitada por defecto, y tenemos que iniciar la herramienta de edición del sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* para hacerlo. Localizaremos la clave *HKEY_CURRENT_USER\Software\Policies\Microsoft\Security* y crearemos o editaremos el valor DWORD existente (CheckAdminSettings), cuyo contenido será 0 para bloquear la ejecución de archivos «.exe» o 1 para utilizar la configuración personalizada de seguridad para este tipo de archivos. Será necesario reiniciar Windows para que los cambios tengan efecto.

33 Solución para los virus de *script*

Intermedio

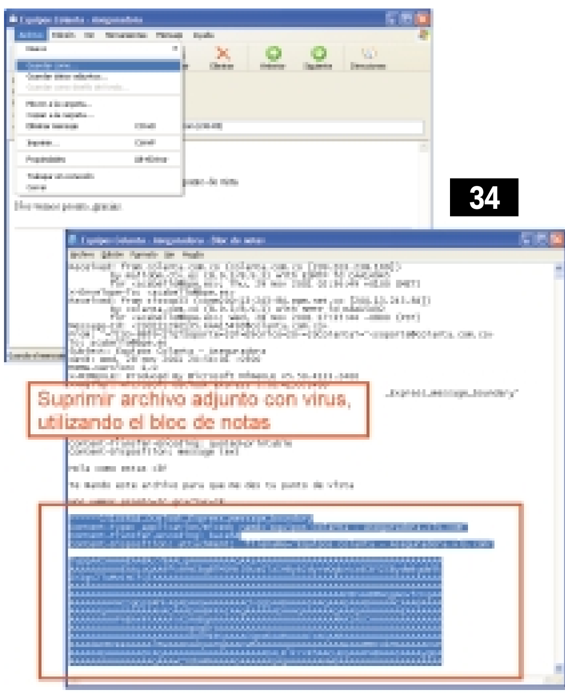


33

Últimamente están proliferando los virus que se expanden a través del correo electrónico como archivos adjuntos y que atacan directamente a nuestra libreta de direcciones, reenviándose los mismos de forma automática a todos los contactos allí almacenados. Este es el caso del famoso virus «I love you». Una solución casera a este problema que envuelve a los peligrosos archivos de *scripting* de Microsoft Visual Basic (aquellos que como extensión tienen las letras «.vbs», «.vbe», «.js», «.wsh» o «.wsf») consiste en modificar la acción predeterminada (aquella que se ejecuta al hacer doble clic) para ver su contenido en el bloc de notas, en vez de correr el código ejecutable que contienen. Para ello es necesario hacer clic con el botón derecho del ratón para ejecutarlo. Esta configuración la realizaremos desde una ventana del explorador de Windows, bajo el menú *Herramientas/Opciones de carpeta/Tipos de archivo* seleccionando la extensión del archivo cuya acción predeterminada modificaremos, seleccionando sus *Opciones Avanzadas*. Sin embargo, la mejor prevención es no ejecutar todos esos archivos que provengan de remitentes desconocidos o no fiables, o que en el nombre del archivo incrustado aparezcan dos extensiones.

34 Eliminar archivos adjuntos de un correo electrónico

Intermedio

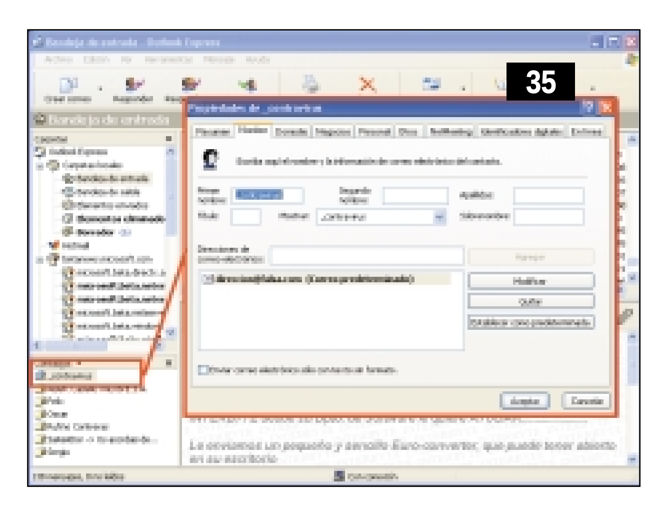


Siguiendo con el problema de los virus incrustados en los mensajes de correo electrónico como archivos adjuntos, podemos encontrarnos con el problema de que un importante mensaje de correo contenga un virus. En ese caso abriremos el mensaje y, dentro de la ventana, abriremos el menú *Archivo/Guardar como*, salvando el mensaje como un archivo «.eml». Acto seguido abriremos este archivo con el bloc de notas («notepad.exe») y nos desplazaremos hasta el principio del código que forma el archivo adjunto, que identificaremos por la cantidad de caracteres de todo tipo que contiene, eliminando todo el contenido hasta el final del mensaje. Guardaremos el archivo y lo arrastraremos hasta la carpeta de Outlook Express que deseemos. La desventaja es que perderemos cerca de dos minutos en realizar esta tarea, pero por el contrario, mantendremos la cabecera original del mensaje de correo.

35 Cómo prevenir la propagación de virus a través de la *Libreta de direcciones*

Intermedio

Cuando corramos el riesgo de ser infectados por uno de estos virus y gusanos, contamos también con otra solución casera pero efectiva. Ésta nos otorgará un poco más de tiempo para desconectarnos de Internet y eliminar todos los mensajes si éstos intentan propagarse a través de la *Libreta de direcciones*. El truco consiste en añadir un nuevo contacto en nuestra

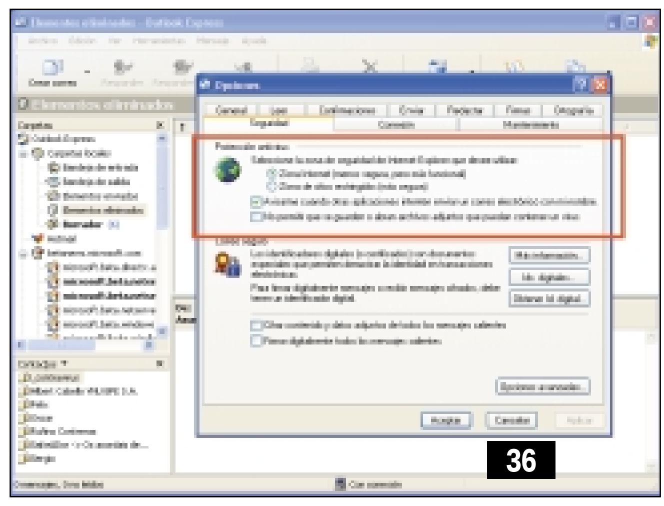


libreta de direcciones que sea el primero en el listado. Para ello, en el campo *Primer nombre* de la ventana *Nuevo contacto* escribiremos «_contravirus» (sin las comillas) y para la dirección de correo electrónico introduciremos una dirección inválida de correo electrónico, como *dirección@falsa.com*. Pulsaremos sobre el botón *Añadir* para crear nuestro nuevo contacto. Lo que ocurrirá es que si un virus o gusano se ejecuta en orden alfabético para reenviarse a sí mismo a todos los contactos existentes en nuestra libreta de direcciones, el primero de ellos será falso, con lo que nos percataremos del problema y podremos solucionar el problema a tiempo.

36 Definir la configuración de zona en la que trabajará Outlook Express

Avanzado

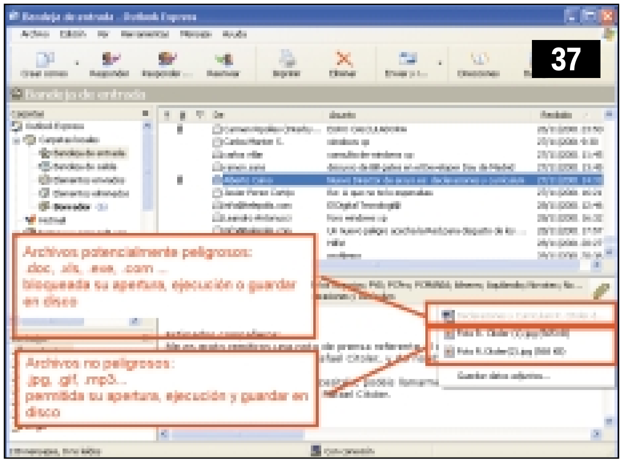
Una de las mayores características de Outlook Express 6.0 son las mejoras relacionadas con la protección contra virus de correo electrónico. Bajo el menú *Herramientas/Opciones* de Outlook Express, en la pestaña *Seguridad,* definiremos la configuración de zona que utilizará Outlook Express durante su funcionamiento (sobre todo con correos electrónicos que utilicen código HTML), que en nuestro caso será «Zonas restringidas (más seguras)». Acto seguido dentro del menú *Herramientas/Opciones de Internet/Seguridad* de Internet Explorer comprobaremos el nivel de seguridad utilizado en las zonas «Internet» y «Sitios restringidos», ya que éstas coinciden con las definiciones de zona de seguridad utilizadas por Outlook



Express, y seleccionaremos las «Zonas restringidas». Eligiendo ésta, todas las opciones de automatización de Outlook Express 6.0 serán desactivadas. Algunos *scripts* invocarán una advertencia sobre controles Active X. De esta forma, si recibimos un correo electrónico con un *scripting* que queramos ver, comprobaremos el código fuente del mensaje, para asegurarnos de que sea seguro. Para evitar los mensajes de advertencia en el panel de *Vista previa* desactivaremos dentro de las opciones de Outlook Express la correspondiente a descargar automáticamente los mensajes al verlos dentro del citado panel, o simplemente desactivaremos esa vista dentro del menú *Ver/Diseño*.

37 Cómo añadir más seguridad para Outlook Express

Avanzado



Contamos además con dos opciones más para aumentar la seguridad de Outlook Express. Se encuentran dentro de la pestaña *Seguridad* y son:

Avisarme cuando otras aplicaciones intenten enviar un correo electrónico con mi nombre, como por ejemplo, casos en los que rellenando un formulario en una página de un servidor web a través de Internet Explorer, estos datos son enviados a través del correo electrónico, pudiendo revelar de esta manera nuestra identidad.

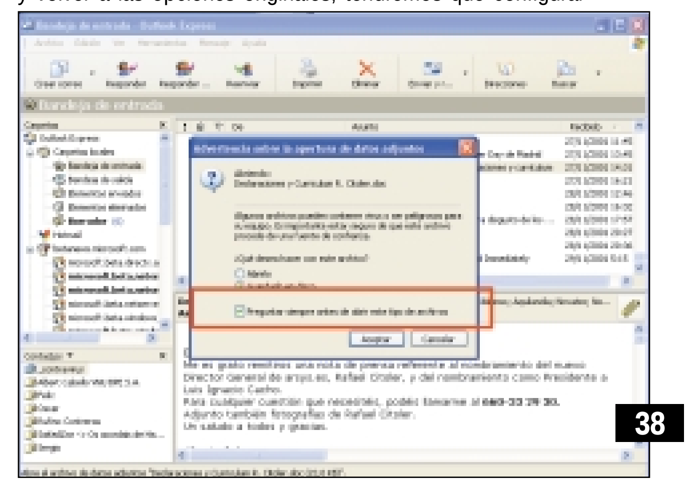
No permitir que se guarden o abran archivos adjuntos que puedan contener un virus. Marcando esta opción desactivaremos la posibilidad de abrir archivos potencialmente peligrosos incrustados en mensajes de correo electrónico, ya que todas las opciones estarán sombreadas impidiendo su apertura, ejecución o la acción de guardarlo en el disco duro. Cuando Outlook Express bloquee un archivo incrustado, en la ventana de mensaje se mostrará un alerta sobre la *Barra de herramientas*, especificando los archivos no seguros bloqueados. Si utilizamos esta opción, para poder ejecutar o guardar un archivo que provenga de algún contacto de confianza tendremos que desactivar temporalmente esta característica.

38 Cómo volver a activar las opciones *Abrir* y *Guardar en disco*

Intermedio

Muchos usuarios de Outlook se preguntarán por qué su cliente de correo ha perdido esta opción cuando hacemos clic sobre un archivo incrustado en un mensaje de correo electrónico. Primeramente, cuando abrimos un mensaje de correo electrónico con un archivo adjunto y seleccionamos ese archi-

vo, Outlook Express nos permite la opción de abrir el archivo, o guardarlo en nuestro disco duro, así como también la posibilidad de definir la opción predeterminada, marcando la casilla *Preguntar siempre antes de abrir este tipo de archivos*. Esta opción, sin embargo, aparecerá sombreada para algunos tipos de ficheros considerados como no seguros por Internet Explorer como los «.exe», para los que tendremos que confirmar su apertura o ejecución. Sin embargo, abrir automáticamente otros tipos de archivos adjuntos no bloqueados por Internet Explorer, como por ejemplo documentos de Word, es potencialmente peligroso, ya que pueden contener macros que infecten nuestro ordenador. Para desactivar esta característica y volver a las opciones originales, tendremos que configurar



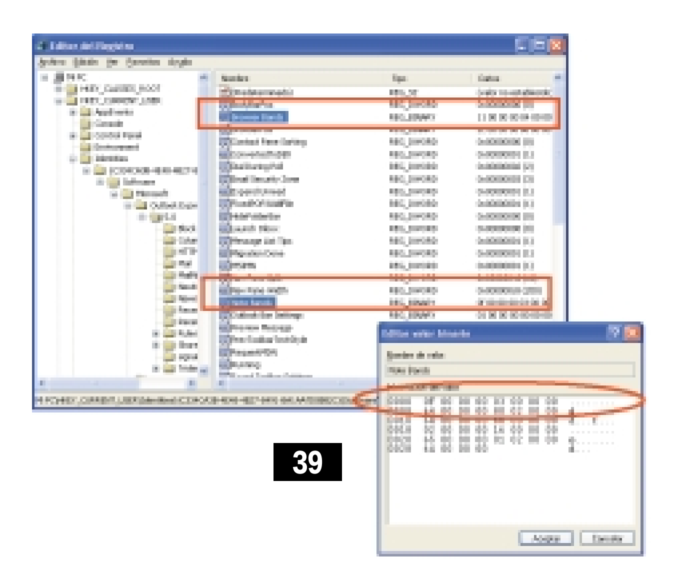
38

un ajuste que se aplica a todo el sistema Windows, ya que una vez desmarcada esta casilla de verificación no existe opción alguna en Outlook Express para devolver este cuadro. En su lugar, abriremos el *Explorador* de Windows y dentro del menú *Herramientas/Opciones de Internet* nos desplazaremos hasta la pestaña *Tipos de archivo* y allí hasta el tipo de archivo registrado que nos está dando problemas, en nuestro caso, el documento de Word. Una vez seleccionadas las *Opciones avanzadas* de este documento, marcaremos la casilla existente en el campo *Confirmar apertura después de la descarga*. Esto restaurará nuestras opciones al abrir archivos adjuntos en Outlook Express.

39 Cómo volver a activar la *Barra de herramientas* y menús que desaparecen

Intermedio

Cuando la *Barra de herramientas* de Outlook Express o alguno de los menús desaparezca, esto puede ser debido a una corrupción en las ramas del registro que componen nuestra identidad. Si bien podemos solucionar este problema creando un nuevo perfil de Outlook e importando los mensajes y la configuración anterior a la nueva, es fácil intentar una última solución. Ésta consiste en iniciar el editor del registro de sistema con el comando «regedit.exe» desde el menú *Inicio/Ejecutar* y localizar la clave *HKEY_CURRENT_USER\Identities\[identificador_de_usuario]\Software\Microsoft\Outlook Express\5.0*. Para devolver a Outlook Express nuestra *Barra de herramientas*, haremos doble clic sobre el valor binario Browser Bands y cambiaremos el quinto número de la primera línea a cualquier otro que no sea 00 01 y 02 para hacer retornar la barra de menús, mientras que con los valores 03 y 04 devolveremos la barra de menús y la *Barra de herramientas*.
Si los problemas de falta de menús nos ocurren en las venta-



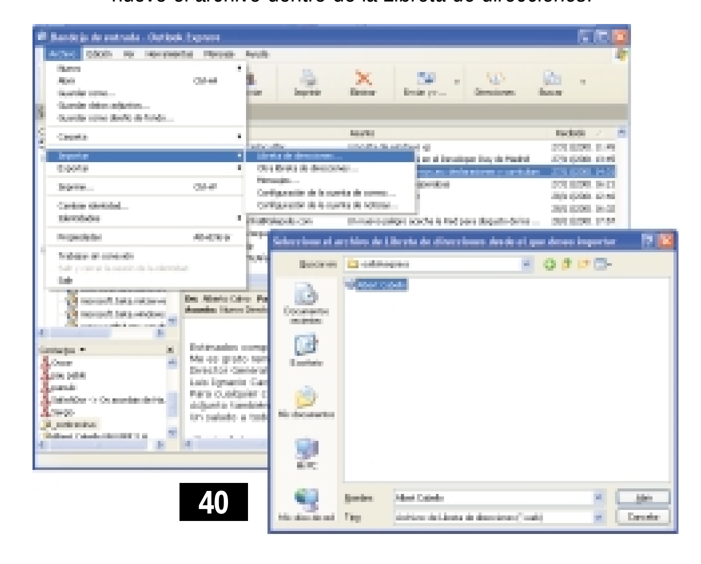
39

nas de composición o respuesta de mensajes, tendremos que realizar estos mismos pasos anteriormente descritos, pero modificando el valor Note Bands y cambiando el valor del cuarto número en vez del quinto.

40 Problemas a la hora de importar archivos «.wab» a otro ordenador

Básico

Comenzando con la versión 5.01 de Outlook Express, la *Libreta de direcciones* de Windows cambió significativamente para añadir soporte Unicode, un juego estándar de caracteres internacionales. Es por esta razón que la compatibilidad hacia atrás está truncada con versiones anteriores de la libreta de direcciones. Si abrimos un archivo «.wab» bajo Outlook Express 5.01 o superior, el archivo será automáticamente convertido para incorporar soporte de Unicode y, por lo tanto, ya no podrá ser leído por OE 5.0, la versión que venía incluida, por ejemplo, en Windows 98. Si desinstalamos Outlook Express y reinstalamos una versión de Windows que no tenga como mínimo la versión 5.01 de Outlook Express, tendremos que copiar nuestra *Libreta de direcciones* a una máquina diferente y exportar nuestros contactos como un archivo de texto de tipo «.csv» (valores separados por comas) e importar de nuevo el archivo dentro de la *Libreta de direcciones*.



40



Netscape 6.2

Nuevas mejoras y plena integración con Windows XP y Mac OS X

Plantarle cara a Microsoft y su Internet Explorer en el mundo de la navegación a través de Internet no es para nada sencillo. Un producto integrado «de serie» en los sistemas operativos de la familia Windows y que además ostenta una enorme calidad se presenta, lógicamente, como una opción más que atractiva de cara al usuario. A pesar de ello, si algún producto puede jactarse de tutear sin complejo alguno a la popular herramienta de la compañía de Bill Gates, ésa es la *suite* Netscape. La versión 6 del navegador de Microsoft aparecía en escena para subir de nuevo el listón y ponerle las cosas más difíciles a la competencia en este sector. Y, obviamente, la reacción del otro gigante no se ha hecho esperar. Netscape 6.2 está aquí, dispuesto a entrar en liza con su más directo rival. Si algo caracteriza a esta nueva versión de la *suite* no es precisamente la carencia de novedades. Más bien todo lo contrario, ya que precisamente sus mejores avales son las muchísimas mejoras que ha asimilado respecto a las anteriores versiones. A lo largo de este capítulo desvelaremos los elementos que han afrontado mayores cambios y aprenderemos a obtener el máximo provecho de ellos. Sin duda alguna y por difícil que parezca, el listón ha vuelto a subir un peldaño.

1 Pasarse a Netscape 6.2

Básico

La pregunta que en primer lugar se harán muchos usuarios de otras *suites* de navegación es: ¿me interesa realmente utilizar esta nueva versión de Netscape? La respuesta inmediata podría ser un rotundo sí, pero en un sector dominado por productos de tanta calidad, lo idóneo es analizar detenidamente qué nos ofrece cada uno de ellos, y decantarse por aquel que más se ajuste a nuestras necesidades. Y no hablamos únicamente de Netscape y Microsoft Internet Explorer, sino que en este grupo de productos de altísima calidad debemos incluir merecidamente a otras herramientas de navegación tan populares como Opera, Vantage o NeoPlanet, analizadas en el volumen anterior del Manual de Trucos y Utilidades Internet. Para facilitar semejante decisión vamos a repasar en primer lugar las principales características que sitúan a Netscape 6.2 como una herramienta muy apetecible para los usuarios de cualquier otro producto de la competencia.



Uno de los aspectos más interesantes de esta *suite* es el elevado grado de personalización que pone al alcance del usuario. Esto se traduce, por ejemplo, en la posibilidad de añadir a la útil *Barra lateral* nuevas pestañas desarrolladas no sólo por Netscape, sino también por terceros. Pero no debemos olvidar la enorme flexibilidad que siempre ha caracterizado a los productos de la compañía, lo que se traduce, por ejemplo, en la posibilidad de automatizar las búsquedas con el motor preferido por el usuario. Otra característica que sin duda agradecerán los usuarios aficionados a utilizar varios sistemas operativos es la portabilidad de Netscape, lo que hace posible utilizarlo no sólo en los sistemas operativos de la familia Windows, sino también en Mac OS y Linux, haciendo totalmente innecesaria la labor de aprendizaje de distintos productos para cada uno de ellos. Pero aquí no acaba todo: es posible rellenar formularios *on-line* de forma automática, gestionar las direcciones de correo electrónico de la forma más sencilla, traducir automáticamente y de forma eficaz páginas web completas, está totalmente integrado con AOL Mail y AOL Instant Messenger, etc. En definitiva, integra suficientes elementos como para satisfacer a los usuarios más exigentes, tal y como iremos descubriendo en los siguientes apartados.

2 ¿Merece la pena actualizar?

Básico

Los usuarios habituales de esta completa *suite* también pueden preguntarse si es realmente interesante actualizar el software instalado en su equipo, máxime si utilizan en la actualidad la versión 6.0 o 6.01. De nuevo, lo mejor que podemos hacer en este caso es repasar las aportaciones que esta nueva ver-



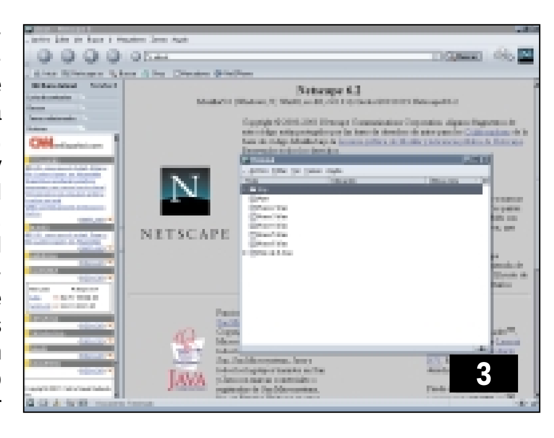
sión hace a las anteriores entregas, de forma que sea cada usuario quien tome la decisión teniendo como base suficientes puntos sobre los que sostenerla. Los cibernautas que tengan instalado en su equipo Netscape 4.x o versiones anteriores disfrutarán de una gran cantidad de mejoras, entre las que destacan: total integración con Windows XP y Mac OS X; gestión simplificada de múltiples cuentas de correo electrónico, entre las que se incluyen AOL Mail, Netscape WebMail o cualquier otro correo IMAP; acceso rápido a los elementos más utilizados a través de la *Barra lateral*; total integración del navegador con la herramienta de correo electrónico, Instant Messenger y Composer; gestión automática de contraseñas para agilizar el acceso a múltiples sitios web; posibilidad de modificar el aspecto de la interfaz a través de los cientos de temas disponibles en Internet y cumplimentado automático de formularios. Todas ellas son tan sólo algunas de las características que la nueva versión ofrece a sus usuarios más veteranos.

Pero las novedades introducidas también las percibirán los cibernautas que tienen instalada en su equipo una de las últimas versiones de esta *suite*. Algunas de las más recientes aportaciones de la versión 6.2 son: gran capacidad de integración con Windows XP, lo que permite al usuario, entre otras cosas, conocer el número de mensajes de correo entrante desde la pantalla de identificación de este sistema operativo; envío de documentos Word, Excel y PowerPoint directamente desde estas aplicaciones a través de la excepcional capacidad de integración del cliente de Netscape Mail con otras herramientas; gran rendimiento y estabilidad; búsqueda sencilla de ficheros descargados en el equipo de forma eficaz y una navegación más eficiente (gracias al nuevo histórico) e inédita herramienta de gestión de marcadores.

3 Requisitos

Básico

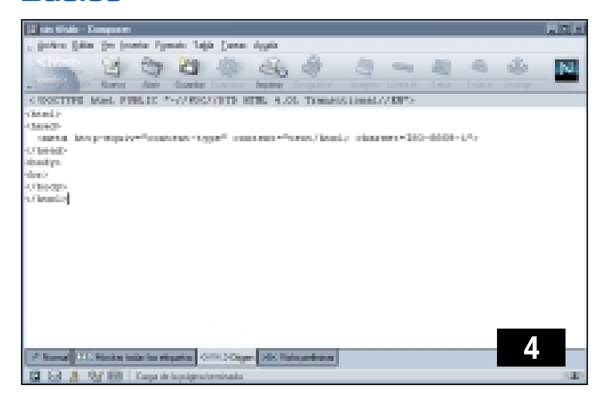
Como hemos mencionado anteriormente, Netscape 6.2 es totalmente compatible con toda la familia Windows actual, con las versiones 8. 6, 9 y X de Mac OS y con Red Hat Linux 6.0, 6.2 y 7.0. Sus exigencias a nivel hardware no son excesivamente elevadas, de hecho todos aquellos usuarios que dispongan al menos de un equipo con microprocesador



Pentium a 233 MHz, 64 Mbytes de RAM y 26 Mbytes de espacio libre en el disco duro pueden utilizarlo. Los poseedores de un Macintosh deberán tener como mínimo un procesador PowerPC 604e a 266 MHz, 64 Mbytes de memoria RAM y 36 Mbytes de espacio libre en disco. Obviamente, unas exigencias razonables que ponen al alcance de un gran número de usuarios la que hoy en día es una de las mejores *suites* de navegación por la Web y gestión del correo electrónico, entre otras funcionalidades.

4 Algo más que Netscape Navigator

Básico

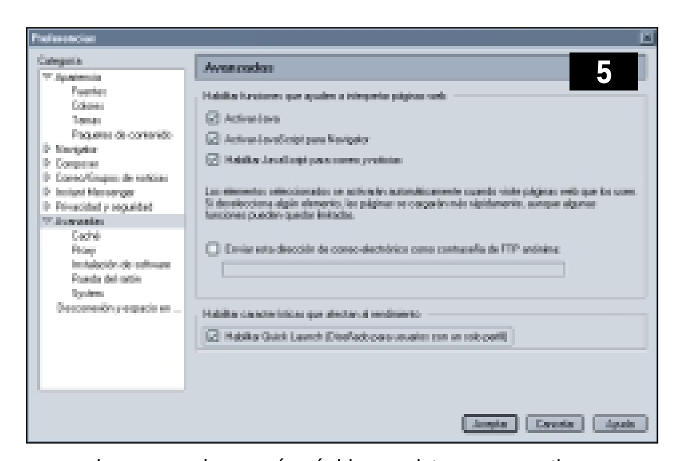


Probablemente, la herramienta más utilizada por la mayor parte de los usuarios de la *suite* es Netscape Navigator. Pero el navegador no es la única aplicación que encontraremos en la última versión del popular producto orientado a la comunidad cibernauta. Para satisfacción de los usuarios más exigentes, acompañando a este eficaz *browser* encontraremos cuatro utilidades más de gran calidad y enorme interés: Netscape Instant Messenger, un gestor de mensajería instantánea muy sencillo de utilizar; Composer, un eficaz editor HTML con el que la creación de páginas web es un poco más asequible gracias, entre otros factores, a la utilización de la tecnología WYSIWYG (*What You See Is What You Get*); Netscape Mail, el popular administrador de correo electrónico y, para finalizar, Netscape Address Book, uno de los libros de direcciones más elaborado y potente que se puede encontrar en la actualidad. Por si todas estas aplicaciones no formasen un paquete lo suficientemente completo y siguiendo la tendencia y necesidades actuales de los usuarios, Netscape 6.2 integra soporte Java, necesario para ejecutar los *applets* tan habituales hoy en día en la Web; RealPlayer 8, para afrontar la reproducción de contenidos multimedia en formato *streaming*; Macromedia Flash, una de las opciones de más arraigada implantación por su versatilidad y el reducido tamaño de los ficheros multimedia que genera; NullSoft WinAmp para llevar a cabo la reproducción de audio en multitud de formatos, de los cuales el MP3 es líder indiscutible; Net2Phone para realizar llamadas a terminales telefónicos convencionales y, por último, Print Plus, una herramienta de Hewlett Packard que facilita enormemente el acceso a servicios de impresión.

5 Inicio rápido

Básico

Uno de los objetivos perennes que tanto los fabricantes de hardware como los desarrolladores de software se han marcado desde los inicios de la informática consiste en reducir los tiempos de espera. Este reto constituye uno de los principales motores de la tecnología informática, de ahí la utilidad de dis-

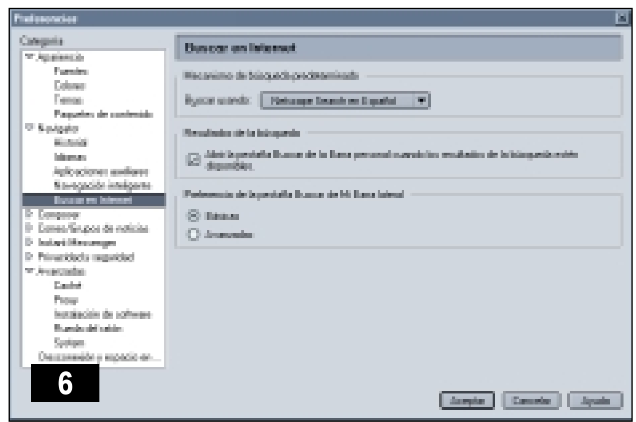


poner de procesadores más rápidos y sistemas operativos más eficaces y ágiles capaces de ejecutar tareas hasta hora impensables por implicar tiempos de proceso desmesuradamente largos. Los responsables de Netscape, conscientes de lo molesto que resulta en ocasiones para el usuario perder un tiempo valioso esperando el inicio de la aplicación, han diseñado una herramienta a la que han bautizado como Quick Launch, y cuya utilidad consiste en reducir drásticamente dicho tiempo de espera. Esta herramienta, disponible únicamente en Netscape para sistemas Windows, brinda al usuario la posibilidad de realizar su activación durante el proceso de instalación, aunque es posible habilitar/deshabilitar Quick Launch en cualquier momento haciendo lo propio con la casilla de verificación ubicada en la categoría *Avanzadas* que encontraremos en la ruta *Editar/Preferencias...*. No obstante, el inicio rápido ha sido diseñado para configuraciones basadas en un único perfil, por lo que no se recomienda su utilización por parte de usuarios que han definido más de un perfil en sus sistemas. Cuando la utilidad Quick Launch se encuentre activada, aparecerá el icono con el logotipo de Netscape en la *Barra de tareas*, junto al reloj. Para iniciar la aplicación tan sólo es necesario hacer doble clic sobre dicho icono. Si lo que deseamos no es iniciar Navigator, sino otro módulo como Composer o el libro de direcciones, basta con acceder al menú contextual de dicho icono haciendo clic en él con el botón derecho del ratón.

6 Opciones de búsqueda

Básico

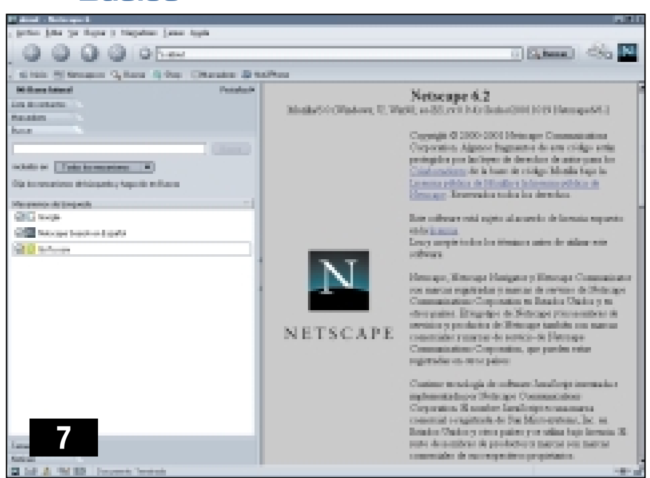
Uno de los principales objetivos de Internet es, por supuesto, la localización de información. Por este motivo, todas las posibilidades que los navegadores ofrezcan a los usuarios con la finalidad de facilitar o agilizar el proceso de búsqueda de todo



tipo de información son siempre bien recibidas. Es precisamente en este terreno donde Netscape se desenvuelve como pez en el agua, poniendo al alcance del usuario múltiples formas de iniciar un proceso de búsqueda: desde la barra de direcciones, utilizando el menú *Buscar* de la aplicación, a través del botón *Buscar* del navegador y, en último lugar, empleando la pestaña *Buscar* de la *Barra lateral*. El resultado de este proceso de búsqueda no se materializa únicamente en la información que aparece en la ventana principal del navegador, ya que la *Barra lateral* también proporcionará al usuario una cantidad importante de información que le permitirá, con tan sólo un clic del ratón, acceder a sitios web alternativos incluso después de la visita de muchas otras páginas de Internet. Por defecto, Netscape 6.2 utiliza el servicio de búsqueda del *Netscape Open Directory Project* y el motor de búsqueda Google. No obstante, es posible personalizar totalmente el mecanismo de búsqueda predeterminado a través de las opciones disponibles en la ruta *Editar/Preferencias.../Navigator/Buscar en Internet*.

7 Búsqueda avanzada

Básico

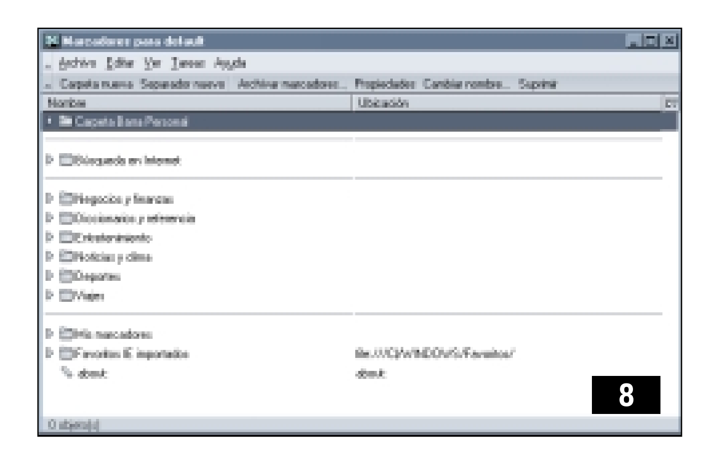


Netscape 6.2 incluye diversas opciones cuya finalidad es maximizar la probabilidad de encontrar la información que buscamos en Internet. Para ello, es necesario establecer la *Barra lateral* en modo avanzado activando el *radio button* etiquetado con la cadena de texto *Avanzadas* ubicado en la ruta *Editar/Preferencias.../Navigator/Buscar en Internet*. Una vez hecho esto, en la pestaña *Buscar* de la *Barra lateral* aparecerán nuevas opciones que nos permitirán utilizar varios motores de búsqueda simultáneamente y establecer categorías de forma realmente sencilla. Gracias a las categorías es posible agrupar motores de búsqueda en función de su eficacia a la hora de encontrar determinados tipos de información.

8 Marcadores

Básico

Los marcadores son un recurso conocido sobradamente por todos los usuarios de Netscape, sin embargo quizás no lo sea tanto el potente gestor a través del cual es posible administrarlos con total libertad. Antes de continuar hablando de estos ingeniosos elementos, debemos recordar que los marcadores no son más que enlaces a páginas web almacenados en el navegador de forma que, para conectarnos a dichas páginas, no sea necesario recordar su URL. Para acceder al gestor de marcadores debemos dirigirnos a la opción de menú *Marca-*

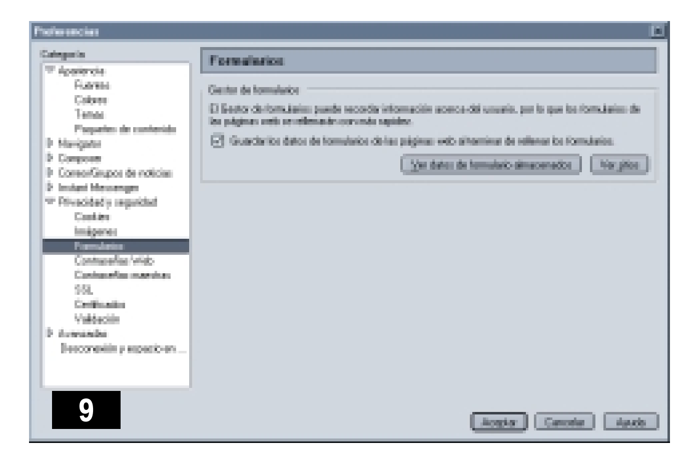


dores/Gestionar marcadores.... Desde aquí no sólo podremos definir nuevos marcadores y eliminar aquellos que no vayamos a utilizar en adelante, sino que también podremos realizar tareas tan interesantes como crear nuevos separadores y carpetas que nos permitan organizar con mayor eficacia nuestros marcadores, importar y exportar archivos de *bookmarks* o realizar búsquedas a partir de la base de marcadores. Pero quizás la opción más interesante sea programar Netscape para que nos avise cuando se actualice el contenido de un sitio web apuntado por un marcador determinado. Para lograrlo, tan sólo hay que acceder al menú contextual del marcador haciendo clic sobre él con el botón derecho del ratón y seleccionando la opción *Propiedades*. A continuación aparecerá una ventana flanqueada por tres pestañas: *Información*, *Programación* y *Notificar*. La primera de ellas únicamente sirve para proporcionar al usuario información acerca del marcador, datos como su nombre y la ubicación de la página web a la que apunta. La segunda pestaña nos va a permitir definir la frecuencia con que deseamos que Netscape verifique si se ha producido la actualización de los contenidos del sitio web apuntado por el marcador. Por último, la pestaña *Notificar* hace posible que el usuario defina la forma en que desea ser avisado por el navegador cuando se produzca la actualización del contenido de alguna de las páginas web apuntadas por un marcador previamente programado.

9 Gestión de formularios

Básico

Son muchas las ocasiones en las que es necesario rellenar amplios formularios durante la navegación en Internet. Cuando contratamos una cuenta de correo electrónico con un nuevo proveedor, realizamos una compra *on-line*, accedemos a información de una base de datos ubicada en la Red, etc., es necesario cumplimentar formularios engorrosos, pero necesarios para llevar a cabo estas tareas. Para facilitar al usuario esta labor, Netscape 6.2 incorpora un completo gestor capaz de rellenar de forma automática todos estos formularios, ahorrando un tiempo valioso al usuario y evitando un esfuerzo innecesario por repetitivo. Una vez cumplimentado un primer formulario, hay dos formas diferentes de introducir en el gestor los datos personales del usuario: utilizando la opción *Guardar datos formulario* del menú *Editar*, o bien respondiendo afirmativamente a la pregunta que el gestor realizará acerca de este asunto una vez que hayamos procedido al envío del formulario. Cuando los datos han sido almacenados en el equipo para ser utilizados en ocasiones futuras, es posible acceder a ellos e incluso editarlos, a través de la categoría *Privacidad y seguridad/Formularios* ubicada en el menú *Editar/Preferencias...*. Para acceder al gestor de formularios basta con hacer clic en el botón *Ver datos de formulario almacenados* ubicado en la ventana que aparecerá tras seguir los pasos indicados anteriormente.

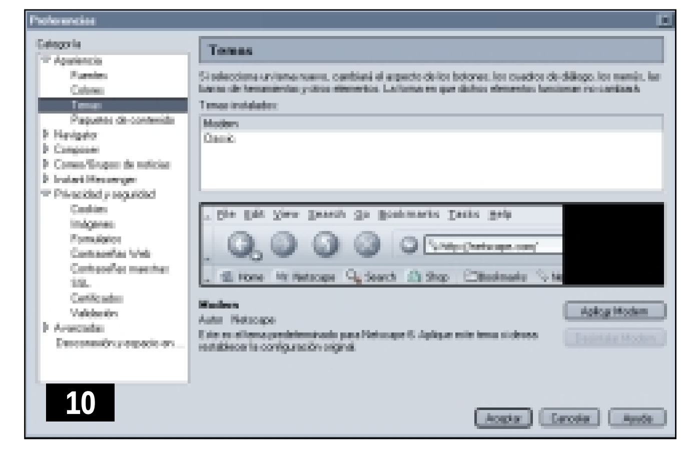


Ahora la pregunta que podemos hacernos es: ¿dónde almacena Netscape todos estos datos? Como es lógico, en un archivo en principio a salvo de posibles intrusos, aunque cabe la posibilidad remota de que alguien no autorizado acceda a dicha información personal. Dado que en este fichero el usuario almacena información vital, como los números de sus tarjetas de crédito, puede ser interesante cifrar su contenido dificultando enormemente su lectura por parte de terceros. La realización de ese proceso está explicada detalladamente en el apartado número 18 titulado «Cifrar información confidencial».

Ahora tan sólo nos queda aprender a utilizar los datos almacenados en el equipo para efectuar el cumplimentado automático de los formularios que nos vayamos encontrando en nuestro deambular a través de la Red. Para ello, una vez que se ha completado la descarga en el navegador de la página que contiene el formulario, nos dirigiremos a la opción *Editar/Rellenar previamente formulario*. Para evitar que un determinado campo se rellene automáticamente tan sólo es necesario anular la selección de la casilla de verificación adjunta a dicho campo.

10 Cambiar el aspecto de la interfaz

Básico



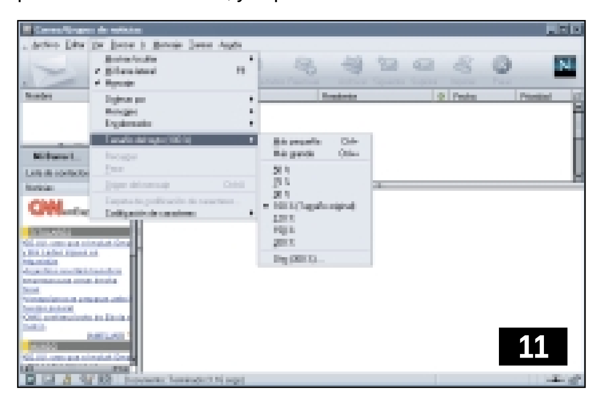
Como viene siendo habitual en este tipo de aplicaciones, Netscape 6.2 permite cambiar radicalmente la apariencia de la interfaz, aplicando tan sólo un nuevo tema de entre los muchos que es posible descargar de Internet (*www.netscape.com/themes*). Para lograrlo, hay que dirigirse a la opción *Editar/Preferencias.../Apariencia/Temas*, seleccionando en la lista el tema que deseemos utilizar. Una forma alternativa de

obtener el mismo resultado consiste en dirigirse al menú *Ver/Aplicar tema*, especificando lógicamente el tema que queremos aplicar. Independientemente del método que utilice el usuario, es necesario cerrar Netscape y volver a iniciarlo para que los cambios tengan efecto.

11 El correo electrónico

Básico

Una de las mejoras más notables que los responsables del desarrollo de la nueva versión de Netscape han introducido en el cliente de correo Netscape Mail ha sido todo lo referente a la integración con otras aplicaciones. Buena muestra de ello es la posibilidad de enviar por correo documentos directamente desde herramientas como Word, Excel o PowerPoint, haciendo tan sólo clic en la opción *Enviar a* del menú *Archivo* presente en todas ellas, y especificando el cliente de correo de



Netscape. En esta nueva versión también se ha simplificado sustancialmente el acceso y gestión de múltiples cuentas de correo permitiendo, por ejemplo, mantener perfectamente separadas la cuenta personal y laboral. Pero las mejoras no acaban aquí: cuando el usuario se disponga a enviar un *e-mail* y se encuentre rellenando el campo *Destinatario*, Netscape propondrá automáticamente una lista de posibles candidatos, tomando como base incluso las direcciones de correo entrante que no han sido almacenadas en el libro de direcciones. Y, para concluir, debemos recordar la posibilidad de incorporar en los mensajes de correo todo tipo de emoticonos, dándoles una apariencia mucho más divertida y afable.

12 Traducción automática

Básico

Por fortuna para todos los hispanohablantes, la fortaleza del español en todos los órdenes de la aldea global está mostrando su influencia en Internet. Ya no resulta extraño comprobar cómo muchas de las páginas más visitadas se encuentran, si no desarrolladas en castellano, sí traducidas a la lengua de Cervantes. Sin embargo, y a pesar de esta buena noticia, la Red sigue estando dominada por la lengua anglosajona, por lo que aquellas personas que se aventuren a navegar a través del ciberespacio y carezcan de unos conocimientos mínimos de inglés, pueden encontrarse con algún que otro problema en determinadas páginas. Es precisamente en estos casos cuando Netscape propone una eficaz solución: traducir íntegramente las páginas al idioma nativo del usuario evitándole el esfuerzo de afrontar por sí mismo el proceso de traducción, o incluso la posibilidad de desechar la información contenida en el sitio web. Utilizar esta funcionalidad del navegador no podía resultar más sencillo: tan sólo hay que dirigirse al menú *Ver* y seleccio-

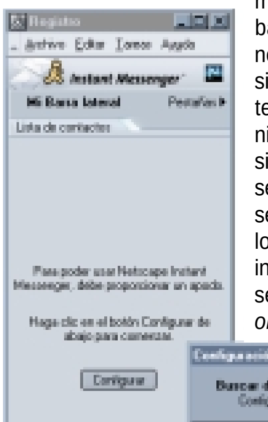


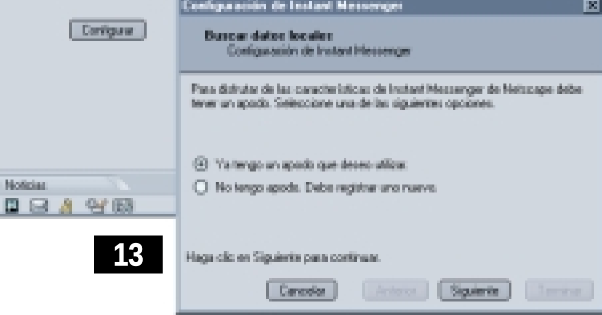
nar la opción *Traducir*. Una vez hecho esto, accederemos a la página web de traducción instantánea, donde el usuario deberá especificar el idioma en el que desea leer el contenido de la página para posteriormente hacer clic en el enlace *Traducir*. El proceso de traducción implica una espera de unos instantes, tras lo cual podremos disfrutar de los contenidos de la página en un español de calidad razonable. Es importante saber que la traducción no será perfecta en ninguno de los casos, pero normalmente sí tendrá la suficiente calidad como para facilitar al usuario la comprensión de los contenidos que allí se exponen.

13 Instant Messenger

Básico

La mensajería instantánea se ha integrado plenamente en Netscape 6.2 gracias a su incorporación a la *Barra lateral* a través de la *Lista de contactos*. De esta forma, es mucho más sencillo y rápido acceder a este servicio desde cualquiera de los distintos componentes que integran la *suite*. Ahora también es posible lanzar una sesión de mensajería instantánea tan sólo haciendo clic en el icono apropiado, presente en numerosas páginas web. Y la que sin duda es la característica más interesante de todas: cuando recibamos un mensaje de correo Netscape nos informará, a través de un icono situado junto a la dirección del remitente, acerca del estado de éste. Esto significa que, en todo momento, sabremos si ese usuario está conectado o no y si se encuentra disponible para iniciar una sesión de mensajería instantánea, por lo que, en caso de estarlo, podremos iniciar, a través de un sencillo clic, dicha sesión y mantener una conversación *on-line* con él.

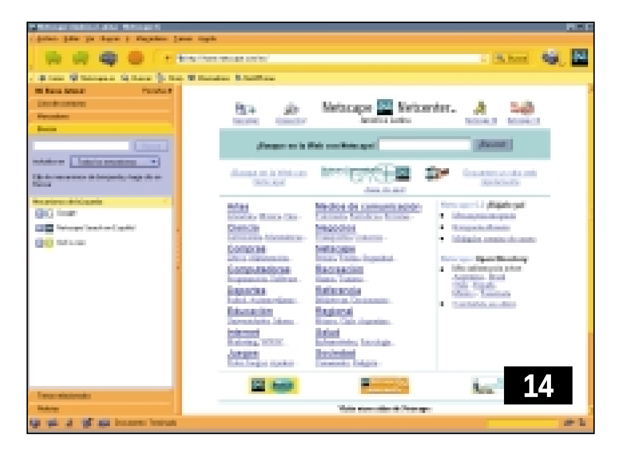




14 Interfaz de usuario mejorada

Básico

Una de las características hacia las que ya apuntaban versiones anteriores de Netscape consiste en la simplificación del aspecto de la interfaz. Para lograrlo, se ha reducido sustancialmente tanto el número de botones como el de barras de herramientas, lo que deja mucho más espacio libre para mostrar las páginas que el usuario descarga de Internet. Una consecuencia adicional de esta simplificación redunda en la sencillez de manejo, tanto aparente como real, de todas y cada una de las aplicaciones que integran la *suite*, lo que facilita notablemente la labor de aprendizaje de aquellos usuarios que han optado por utilizar Netscape para hacer sus primeros pinitos en la navegación a través de Internet.

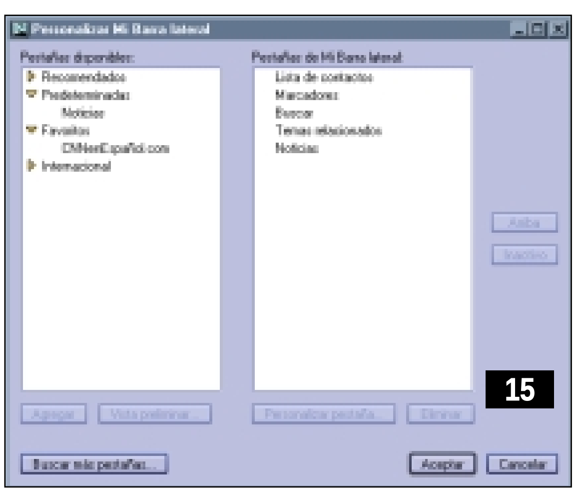


Como hemos comentado en el apartado 10, es posible cambiar el aspecto de la interfaz de forma sencilla. No obstante, esta decisión es más importante de lo que en un principio puede parecer, ya que afecta de forma determinante a la ergonomía de la aplicación. Esta influencia se manifiesta básicamente en los colores y tamaño de los botones por lo que, dependiendo del tema activo, en un momento dado la utilización de la herramienta puede ser más o menos placentera. Este factor se vuelve mucho más importante cuando son personas con deficiencias visuales quienes van a emplear la aplicación. Por este motivo, es realmente importante seleccionar no sólo el tema que otorgue una apariencia, en opinión del usuario, más bonita a la aplicación, sino aquel con el que le resulte más cómodo trabajar. Una buena forma de comprobar las importantes diferencias que existen a este nivel entre unos *skins* y otros es aplicar consecutivamente los dos que integra la *suite* por defecto: *modern* y *classic*. Mientras el primero está gobernado por botones de gran tamaño y colores de agradable tono pastel, el segundo alberga iconos de reducidas dimensiones y colores más vivos.

15 Ampliar la *Barra lateral*

Básico

La *Barra lateral* constituye una útil herramienta capaz de agilizar enormemente el acceso a determinadas funciones de la *suite*, haciendo innecesaria la utilización de menús y demás elementos que en ocasiones penalizan la productividad del usuario. Realmente la *Barra lateral* no es más que un marco en el que los consumados cibernautas pueden encontrar información actualizada acerca de los últimos acontecimientos, motores de búsqueda agrupados por categorías, sus marcadores favoritos, la lista de contactos desde la cual iniciar

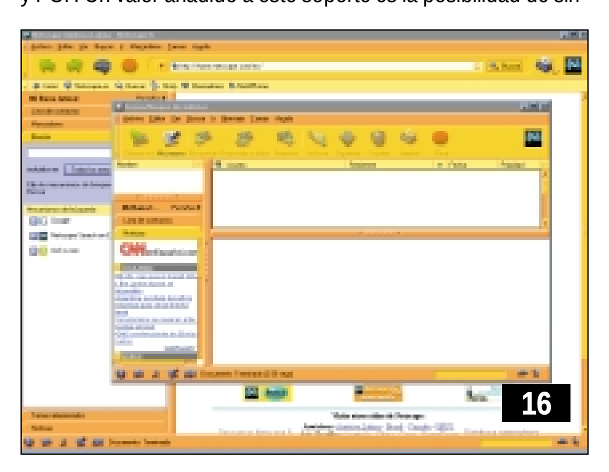


sesiones de mensajería instantánea, etc. Por supuesto, las diferentes pestañas que integran la *Barra lateral* son totalmente personalizables, lo que permite al usuario decidir cuáles desea que formen parte de dicha barra y cuáles no. Y aún más, en Internet se pueden encontrar multitud de pestañas que cualquier usuario puede descargar e instalar en su navegador, no sólo desarrolladas por Netscape, sino también por terceros. Los ámbitos de estos elementos abarcan todo lo imaginable: desde pestañas que albergan todo tipo de información musical hasta aquellas en las que se nos informa acerca de las previsiones meteorológicas. Para buscar nuevas pestañas con las que ampliar la funcionalidad de la *Barra lateral* no hay más que dirigirse a *Mi Barra lateral/Pestañas/Personalizar Mi Barra lateral...*. A continuación tan sólo será necesario hacer clic en el botón *Buscar más pestañas...* para iniciar el proceso de localización. La instalación de estos ingeniosos elementos en nuestro navegador no podía ser más sencilla: únicamente hay que hacer clic en el icono *Add tab to Netscape 6* presente en la mayor parte de las páginas web que ofrecen la descarga de pestañas para proceder a su instalación de forma automática.

16 Múltiples cuentas de correo

Básico

En esta nueva versión de Netscape se ha simplificado notablemente la administración de varias cuentas de correo de forma simultánea y por parte del mismo usuario. La *suite* ofrece soporte íntegro de cuentas de correo Netscape WebMail, AOL Mail y de cualquier otra cuenta que utilice los protocolos IMAP y POP. Un valor añadido a este soporte es la posibilidad de sin-

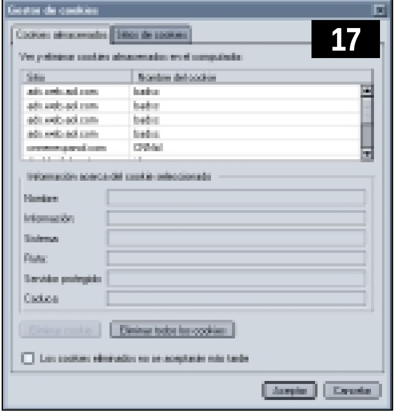


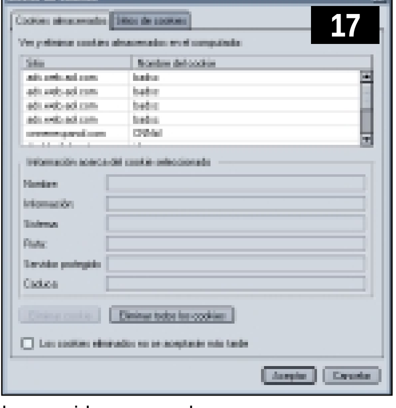
cronizar los libros de direcciones de cuentas AOL y Netscape WebMail, además de permitir a los usuarios de este último proveedor gestionar su cuenta de correo *off-line*, lo que les permitirá prescindir de la conexión en ciertos momentos.

17 Gestionar las *cookies*

Intermedio

Las *cookies* son uno de los recursos utilizados por muchos servidores web para almacenar información acerca de los usuarios que se conectan a ellos. Su finalidad principal es conocer las preferencias de los usuarios de forma que, cuando éstos se conecten al servidor en cuestión, sean identificados de acuerdo a su perfil y se puedan tomar distintas decisiones en lo referente a sus predilecciones que faciliten la navegación a través de las páginas del servidor en cuestión. Las *cookies* son realmente pequeños ficheros que se almacenan en el propio ordenador del cliente, y que son consultados por los servidores cuando éste se conecta. Como hemos visto su utilidad es clara, pero por desgracia un ingenioso elemento ideado para facilitar la navegación a los cibernautas puede volverse una amenaza. La explicación es que el usuario no conoce en primera instancia la información que alberga una *cookie*, por lo que nada impediría que en su interior almacenase información que el usuario desea preservar de terceros no autorizados. Para solucionar este problema, Netscape incorpora un completo gestor de *cookies* que permite al usuario no sólo eliminar de su equipo aquellas susceptibles de ser potencialmente peligrosas, sino también especificar qué servidores tienen permiso para utilizarlas y cuáles no. Todas estas opciones están disponibles en la ruta *Tareas/Privacidad y Seguridad/Gestor de cookies*. Para bloquear o desbloquear las *cookies* de un servidor web determinado es necesario conectarse en primer lugar a dicha página, para a continuación hacer clic en la opción apropiada que encontraremos en la ruta especificada anteriormente. La opción *Ver cookies almacenados* muestra, además de un listado con todas las almacenadas en la máquina, una relación con todos los sitios web responsables de su creación, así como distinta información acerca de cada uno de los ficheros, como la fecha de caducidad o su ruta.

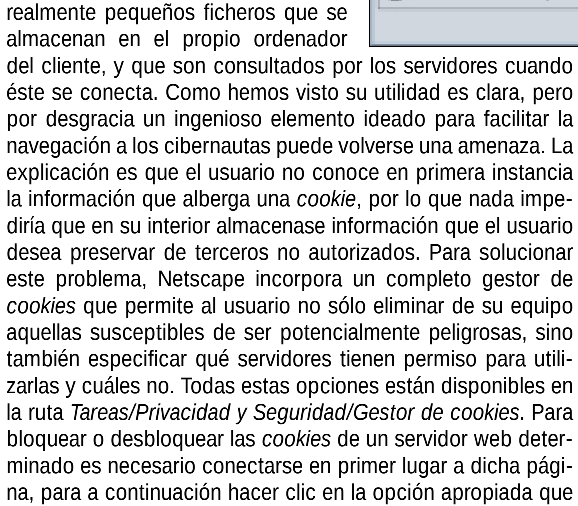




18 Cifrar información confidencial

Básico

Como hemos visto en los apartados anteriores, Netscape integra diversos gestores susceptibles de albergar importante información acerca de los usuarios. Dos son los que destacan en este apartado: el gestor de contraseñas y el de formularios. Como es natural, es altamente recomendable utilizar algún medio de seguridad que proteja dicha información relevante del acceso de usuarios no autorizados. Para solucionar esta problemática se utiliza el cifrado, que no es más que un método algorítmico que transforma una determinada información en otra a priori ininteligible por todos aquellos que no conozcan la clave de cifrado o maestra. La información susceptible de ser cifrada es toda aquella que pueda ser utilizada por terceros de forma fraudulenta, como números de tarjetas de crédito, contraseñas de correo electrónico, claves de páginas web, etc. Y aquí es precisamente cuando aparece en escena la contraseña maestra. Esta nueva clave forma parte del dispositivo de seguridad por software integrado en Netscape 6.2 y su principal función es proteger la clave maestra que hemos mencionado anteriormente.



A través del gestor de contraseñas ubicado en la ruta *Tareas/Privacidad y seguridad/Gestor de contraseñas* podremos ver las contraseñas almacenadas en el equipo, cambiar las claves maestras y encriptar / eliminar la información confidencial. Pero además desde este mismo módulo de la *suite* es posible determinar si queremos que Netscape recuerde las contraseñas y los nombres de usuario requeridos por algunos servidores web, de forma que sea la aplicación la encargada de rellenar estos campos de forma automática. Para ello, cuando se efectúe la conexión a un servidor que requiera identificación previa, el gestor de contraseñas mostrará un cuadro de diálogo preguntando al usuario si desea almacenar tanto el nombre de usuario como la contraseña, en previsión de futuros accesos a dicho sitio web.



NetCaptor 6.5

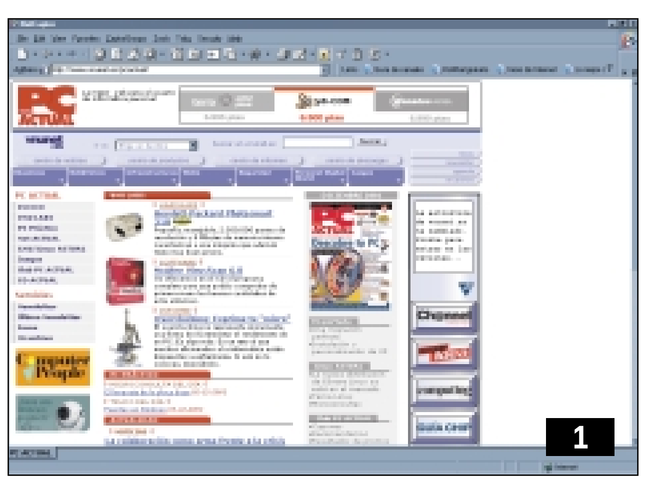
Descubre las interesantes características de este navegador / CD

En el volumen anterior del «Manual de Utilidades y Trucos Internet» dedicamos varios capítulos a algunos de los navegadores que pretendían enriquecer el panorama dominado en un principio por Microsoft y Netscape. Vantage, Opera o NeoPlanet, entre otros, ofrecían características más que interesantes, perfectamente capaces de atraer la atención de un amplio espectro de usuarios y renovar un segmento marcado por los dos gigantes anteriormente mencionados. En esta ocasión vamos a prestarle una parte de nuestro espacio a NetCaptor, un navegador no muy popular pero con calidad más que suficiente para hacerse un hueco en un sector repleto de proposiciones más que interesantes.

1 Una interfaz típica pero eficaz

Básico

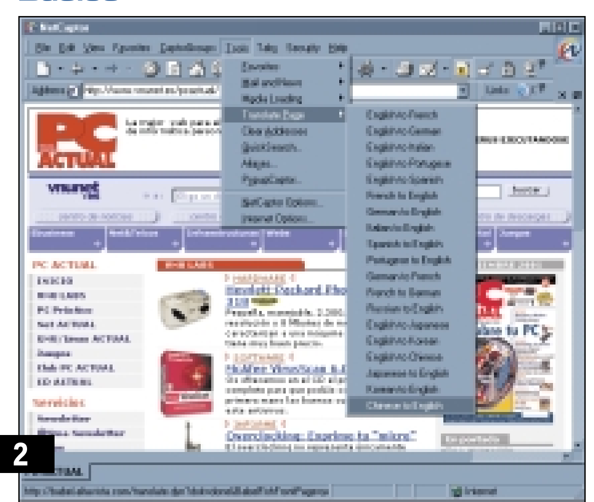
La omnipresente plataforma Windows deja pocas posibilidades de innovación en lo que concierne al aspecto de la interfaz de las aplicaciones. Este es el motivo de que una vez concluido el proceso de instalación del navegador pensemos que estamos ante uno más de tantos. Sin embargo, no es conveniente tomarse tan a la ligera esta primera toma de contacto. A pesar de contar con una interfaz que apenas difiere de lo visto hasta la fecha, NetCaptor incluye opciones lo suficientemente atractivas como para tenerlo en cuenta a la hora de elegir nuestro *browser* favorito. Debemos ser conscientes de que la recurrencia a una fórmula tantas veces vista redunda en una mayor familiaridad, lo que permite al usuario personalizar y comenzar a utilizar la herramienta de inmediato.


1

Lo primero que suele hacer todo usuario que se dispone a descubrir un nuevo navegador es introducir una URL en la barra de direcciones apropiada. Una vez hecho esto, podremos descargar en nuestro equipo sucesivas páginas web con una importante diferencia respecto a otros navegadores más populares: el resto de páginas se descargan como instancias dentro de la misma aplicación. Esto implica que no veremos multitud de ejemplares del mismo navegador en nuestra *Barra de tareas*, sino un único navegador con múltiples instancias en su interior. Para utilizar esta característica no tenemos más que dirigirnos a la opción *File/New Browser/Blank*. Si queremos colocar en primer plano una de estas páginas no tenemos más que hacer clic con el ratón encima de la pestaña apropiada de entre las que encontraremos en la esquina inferior izquierda de la interfaz.

2 Abajo barreras idiomáticas

Básico

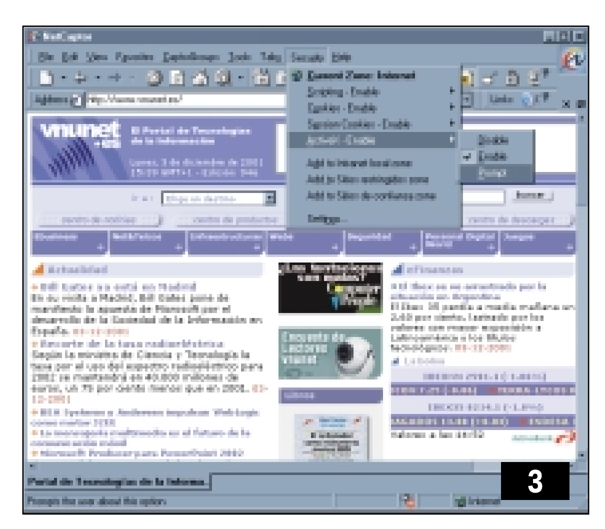

2

A estas alturas parece poco probable que alguien llegue a extrañarse de la indudable supremacía que, muy a pesar de los hispanohablantes, ostenta la lengua anglosajona en Internet. Conocer a un nivel al menos elemental el idioma de Shakespeare es condición imprescindible si queremos obtener el máximo provecho de nuestras incursiones en la Red y, por desgracia, este requisito no está al alcance de todo el mundo. Pero, por fortuna, no es estrictamente necesario afrontar un curso de inglés acelerado si queremos culminar con éxito nuestra relación con Internet. Para deleite de los usuarios que no conocen esta lengua, NetCaptor integra una herramienta

de traducción de páginas web razonablemente eficaz que nos va a permitir descifrar esa información en un principio incomprensible. En realidad lo que la aplicación hace es recurrir a uno de los traductores más eficaces que podemos encontrar en la Web: el integrado en AltaVista (*www.altavista.com*). Para aprovecharlo tan sólo tenemos que dirigirnos, una vez cargada la página que deseamos traducir, a la opción *Tools/Translate Page*. Las posibilidades son enormemente amplias, no restringiendo las opciones a la habitual traducción de lengua inglesa a español, algo que agradecerán los políglotas consumados. De hecho, podremos leer nuestras páginas favoritas en lenguas tan exóticas como japonés o coreano. Su utilidad, como es obvio, depende de los conocimientos idiomáticos del internauta.

3 Seguridad a flor de piel

Básico

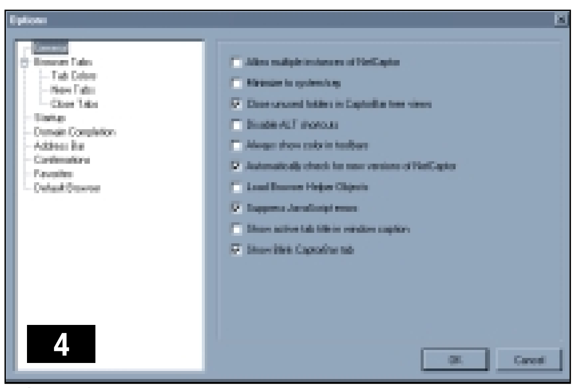


Las opciones que permiten a los usuarios personalizar el comportamiento de su navegador en todo lo concerniente a la seguridad no deben menospreciarse. Como ejemplo, las *cookies*, una sencilla herramienta ideada en principio para facilitarnos nuestro acceso a determinadas webs recordando, entre otros datos, nuestras preferencias, pueden tornarse en peligrosas utilidades capaces de suministrar información privada a terceros. Por este motivo, es de vital importancia configurar el comportamiento del navegador de forma que se adecue a nuestras necesidades y exigencias. Las posibilidades de NetCaptor en este sentido son amplias: es posible deshabilitar la utilización de las mencionadas *cookies*, la ejecución de *scripts* que puedan en potencia llevar a cabo tareas cuanto menos «sospechosas», etc. Para lograrlo, tan sólo tendremos que dirigirnos a la opción de menú *Security* y activar o desactivar cada uno de los parámetros de acuerdo a nuestras preferencias.

4 Configuración general

Intermedio

NetCaptor ofrece la posibilidad de personalizar su comportamiento de forma sencilla a través de las opciones disponibles en el menú *Tools/NetCaptor Options*. El comando de configuración general nos brinda la posibilidad de definir una amplia variedad de parámetros relativos al comportamiento de la herramienta en primera instancia, activando tan sólo las casillas de verificación adecuadas. Las posibilidades son enormemente amplias, ya que podremos permitir la creación de

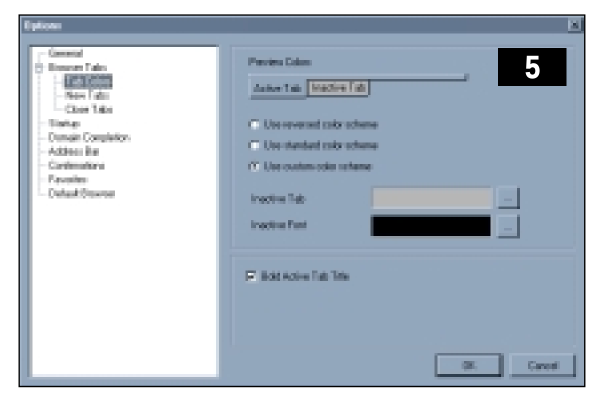


múltiples instancias del navegador, desactivar los accesos directos utilizando la tecla «Alt» o inhibir los errores JavaScript que se produzcan, entre otras muchas opciones.

5 Manipulando instancias

Intermedio

En la ruta *Tools/NetCaptor Options/Browser Tabs* encontraremos las opciones que nos permitirán manipular el comportamiento de las distintas instancias que tengamos abiertas en nuestro navegador. Como instancia entenderemos cada una de las diferentes páginas web que hayamos descargado,

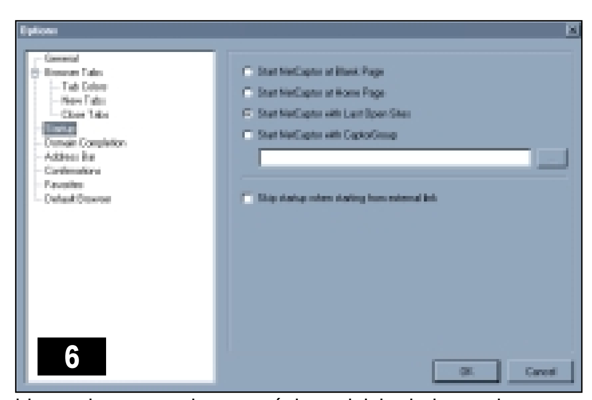


teniendo en cuenta que NetCaptor por defecto integra todas ellas en su interior, por lo que no las localizaremos en la *Barra de tareas* del sistema operativo, sino en las pestañas que encontraremos en la parte inferior izquierda de la herramienta. Desde la ruta anteriormente mencionada podremos personalizar el color de las pestañas de las instancias inactivas, definir la forma de cerrar cada una de ellas o especificar qué página se descargará cuando iniciemos una nueva instancia a través de la combinación de las teclas «Ctrl + N», entre muchas otras posibilidades. Todo esto lo lograremos haciendo clic con el puntero del ratón en la casilla de verificación o *radio button* adecuado.

6 Afinar el navegador

Intermedio

En los dos apartados anteriores hemos explicado algunas de las más importantes características personalizables por el usuario que podemos encontrar en el navegador. Sin embargo, las posibilidades de configuración no acaban aquí, ya que la ventana de opciones de personalización muestra seis adicionales que aún no han sido tratadas. A través del parámetro *Startup* es posible definir qué página debe cargar la aplicación cuando ésta se inicia. Las posibilidades son múltiples: es via-

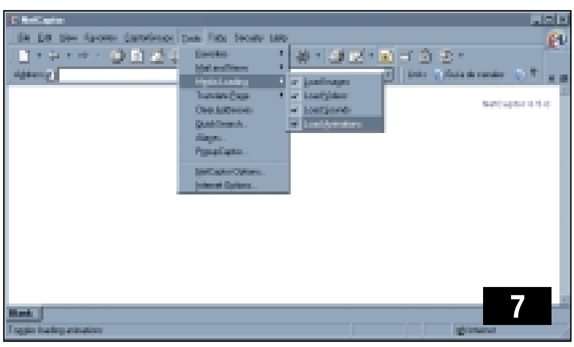


ble no descargar ninguna página e iniciar la herramienta con una página en blanco, también puede mostrar una página por defecto o incluso es posible cargar la última página visitada.
Otra opción que NetCaptor pone a disposición del usuario es *Domain Completion*, una herramienta muy útil que agiliza notablemente la escritura de la URL en la *Barra de direcciones*. Gracias a ella es posible omitir el nombre de dominio cuando se escribe la dirección web, ya que mediante la pulsación de la serie de teclas que vemos en la ventana de opciones daremos la orden al navegador de que escriba el nombre de dominio adecuado.
Las restantes ventanas de configuración que encontraremos en la opción *Tools/NetCaptor Options/Browser Tabs* nos permitirán especificar si deseamos que NetCaptor sea el navegador por defecto. Además, podremos decidir si queremos que la aplicación muestre el habitual botón *Go* junto a la *Barra de direcciones* e incluso será posible activar las ventanas emergentes de confirmación durante la sesión de trabajo.

7 Optimizar la conexión

Básico

Sacar el máximo partido de nuestra conexión a Internet es ahora posible gracias al alto nivel de personalización que este navegador pone a disposición del usuario. Los muchos aficionados al ciberespacio que aún no disponen de una conexión a la Red de banda ancha conocen sobradamente las limitaciones que imponen los módems convencionales que operan sobre el vetusto par trenzado de la línea telefónica clásica. El tiempo que tarda una página en cargar en nuestro navegador y aparecer ante el usuario es directamente proporcional a su tamaño, y los contenidos que más «inflan» una página son precisamente los ficheros gráficos, sonidos, vídeos y animaciones. Cuando una página contiene alguno o varios de estos elementos, el tiempo que tarda en llegar a nuestro ordenador aumenta considerablemente, llegando en ocasiones a hacerse insufrible. Para evitar la descarga de este contenido adicional tan sólo es necesario recurrir a la opción ubicada en el menú *Tools/Media Loading*. Aquí encontraremos cuatro casillas de

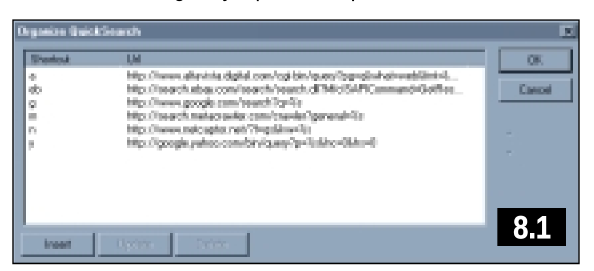


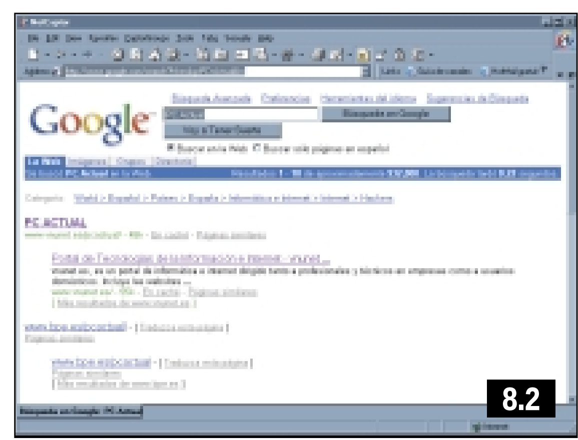
verificación a través de las cuales podremos determinar si deseamos impedir que estos contenidos se descarguen en nuestro equipo desde Internet, con el consiguiente ahorro de tiempo que esto ocasiona, tal y como hemos visto.

8 Motores de búsqueda

Básico

Sin lugar a dudas, los buscadores son las páginas más utilizadas por los cibernautas en su navegación a través de la Red. Localizar la información adecuada acerca de cualquier materia es realmente sencillo gracias a estas eficaces herramientas. Sin embargo, si lo pensamos fríamente, es mucho el tiempo y el esfuerzo que un usuario invierte en teclear en la *Barra de direcciones* la URL del buscador, para a continuación especificar la clave de la búsqueda y hace clic en el botón que inicia todo el proceso. Evitar esta tarea farragosa y repetitiva es posible a través de la cre-



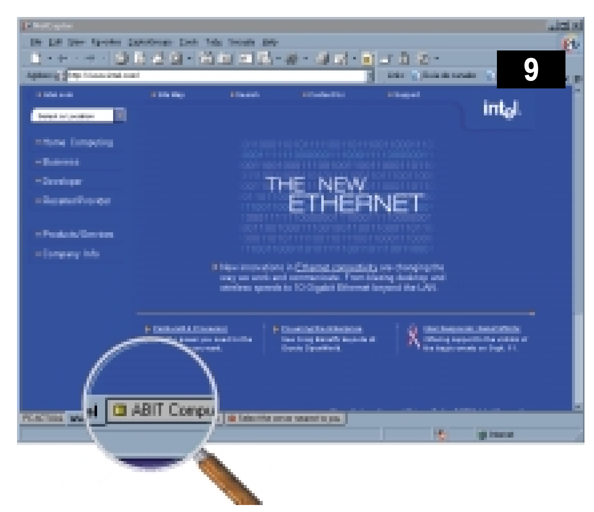


ación de accesos directos que podemos utilizar directamente desde la *Barra de direcciones* de NetCaptor. De esta forma el usuario puede iniciar búsquedas utilizando sus motores de búsqueda favoritos de forma mucho más rápida que si utilizase el método convencional. Para lograrlo, es necesario dirigirse a la opción de menú *Tools/QuickSearch*. A continuación haremos clic en el botón *Insert*, lo que hará aparecer en la ventana dos nuevos campos en blanco que deberemos rellenar: uno en el que especificaremos la URL y patrón de búsqueda de nuestro motor favorito y otro en el que se definirá el nombre del acceso directo. El nombre de este último (campo *Shortcut*) puede ser cualquiera que pueda ser asociado fácilmente con el motor de búsqueda en cuestión. Sin embargo, para rellenar el otro campo, identificado por la cadena *URL*, deberemos iniciar otra instancia del navegador, teclearemos en la *Barra de direcciones* la dirección web del buscador y posteriormente iniciaremos una búsqueda al azar. Cuando ésta haya concluido, nos dirigiremos a la *Barra de direcciones* y comprobaremos cómo la URL ha sufrido modificaciones, ya que ahora es sustancialmente más extensa que antes de iniciar la búsqueda. Tan sólo tendremos que copiar esta dirección, marcándola con el ratón y pulsando la combinación de teclas «Ctrl + C», para pegarla a continuación presionan-

do las teclas «Ctrl + V» en el campo *URL* de la ventana *Quick-Search* de NetCaptor, no sin antes sustituir la palabra que hemos utilizado como clave de la búsqueda por los caracteres *%s*. Para utilizar el alias que acabamos de definir tan sólo será necesario teclear en la *Barra de direcciones* de NetCaptor en primer lugar el nombre del acceso directo que introdujimos anteriormente en el campo *Shortcut*, para a continuación y separados por un espacio, especificar la clave de la búsqueda que deseamos realizar. NetCaptor incorpora una serie de alias predefinidos que es posible utilizar desde el primer momento, ahorrándonos todo este proceso. Como ejemplo, si deseamos buscar en Internet información sobre los mapaches utilizando el buscador Google, introduciremos la siguiente cadena de caracteres en la *Barra de direcciones*: *g mapaches*.

9 Indicadores de estado

Básico

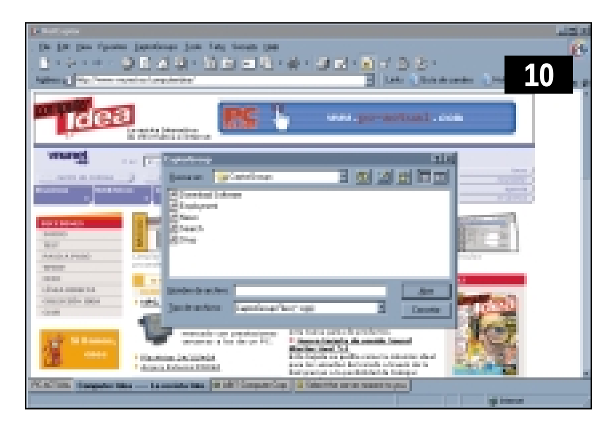


NetCaptor permite conocer en todo momento el estado de cada una de las instancias que hayamos iniciado en el navegador. Como hemos comentado anteriormente, para situar una de estas instancias en primer plano en la aplicación tan sólo tenemos que hacer clic sobre la pestaña apropiada ubicada en la parte inferior izquierda de la ventana de la herramienta. Y es precisamente en esa pestaña donde encontraremos un indicador luminoso cuya finalidad es informar al usuario del estado de descarga de la página web. Este elemento adoptará un color rojo durante el intento de conexión, para posteriormente volverse amarillo durante la fase de descarga. Conocer el significado de estos indicadores de estado es muy útil cuando se han iniciado varias instancias de descarga, ya que nos permiten tener en primer plano una página cuya carga se ha completado totalmente conociendo en todo momento el estado de las demás, pudiendo colocar en primer plano aquella que interese justo en el momento en que concluya su descarga.

10 Organización ante todo

Básico

Recordar la dirección de una página descubierta por azar puede ser una ardua tarea, máxime teniendo en cuenta la cantidad de webs interesantes que proliferan en la Red. Para resolver este problema la mayor parte de los navegadores permiten almacenar las URL facilitando posteriormente la recuperación de la forma más simple. NetCaptor no sólo permite realizar esta tarea, sino también gestionar las direcciones web de forma eficaz a través de los *CaptorGroups*. Cada *CaptorGroup*

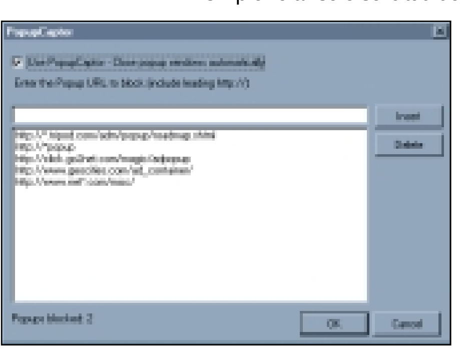


contiene una lista de enlaces a sitios web que es posible iniciar tan sólo haciendo clic sobre el grupo en cuestión. Para definir nuevos *CaptorGroups*, añadir enlaces a cualquiera de ellos o modificarlos es necesario dirigirse al menú *CaptorGroups* y seleccionar la opción adecuada. Para añadir un enlace a un grupo nos decantaremos por la opción *Add to CaptorGroup...* Si lo que queremos es agrupar un conjunto de enlaces en un mismo grupo descargaremos las respectivas páginas web en otras tantas instancias y utilizaremos la opción *Save as CaptorGroup...* Finalmente, para modificar el contenido de un grupo utilizaremos la opción *Organize CaptorGroup…* Como vemos, es una forma de gestionar las direcciones web almacenadas en nuestra máquina de forma similar a las utilizadas por otras herramientas como Netscape.

11 Deshabilitar las ventanas emergentes

Intermedio

Uno de los elementos que contribuye en muchas ocasiones a hacer desesperante la navegación por la Web, sobre todo cuando no se dispone de una conexión de banda ancha, son las ventanas emergentes. Son muchos los sitios web que instancian automáticamente nuevas ventanas, normalmente repletas de publicidad, sin previo aviso o solicitud de permiso por parte del usuario. Aunque en un principio puede parecer que con cerrarlas se soluciona el problema, no es así, ya que el tiempo invertido en descargar el contenido de estas ventanas podría haberse ahorrado invirtiendo el caudal de información de éstas en descargar la página que realmente nos interesa. Para solucionar este hándicap de forma eficaz NetCaptor implementa una herramienta denominada *Capturador de ventanas emergentes*. Gracias a esta utilidad el usuario puede especificar qué URL carece de permiso para instanciar nuevas ventanas por su cuenta. Para llevar a cabo esta tarea deberemos dirigirnos al menú *Tools/PopupCaptor…* Tras hacer clic sobre este comando, aparecerá una nueva ventana en la que podremos introducir las direcciones web que deseamos bloquear. Para ello tan sólo hay que escribir la URL completa en el campo apropiado, incluyendo el protocolo utilizado. A continuación tan sólo tendremos que hacer clic sobre el botón *Insert* para añadir esta dirección a la lista de URL bloqueadas. Un ejemplo sería: *www.pc-actual.com*. Es necesario comprobar que la casilla de verificación etiquetada con la cadena *Use PopupCaptor – Close popup windows automatically* se encuentra activada si deseamos que esta herramienta cumpla su función.



11



Microsoft FrontPage 2002

Optimiza el uso de este editor de HTML

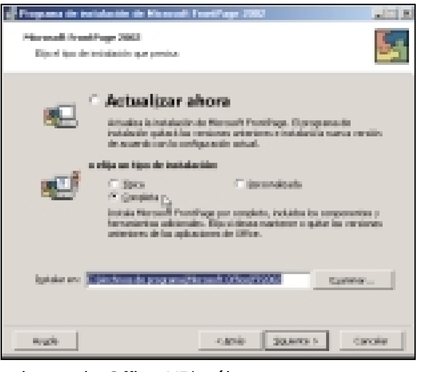
La herramienta de creación de páginas web diseñada por Microsoft se consolida en Office XP con un aspecto más remozado –más juvenil- y una estabilidad que supera a la de las versiones precedentes. Por ello, es de suponer que quienes aún trabajen con Office 95 o 97 se planteen muy en serio si ya ha llegado la hora de proceder a una actualización. No obstante, los usuarios de la versión 2000 deberán plantearse de forma muy clara si realmente se justifica el cambio.

El motivo es que las mejoras de funcionalidad no son tan espectaculares como podría pensarse a priori (aunque a estas alturas ya son pocos los programas capaces de sorprendernos con nuevas versiones, dado que resulta difícil mejorar lo que ya de por sí resulta satisfactorio), pero incluso así la sensación general es que el producto ha madurado un poquito más.

1 Instalar o actualizar

Básico

No sabemos si es debido a las razones apuntadas en los párrafos previos, lo cierto es que a la hora de instalar FrontPage 2002, que se entrega en forma de CD-ROM separado (junto con otro CD-ROM de MS Publisher) en la versión Professional de Office XP, al usuario se le ofrece la posibilidad de actualizar su sistema (obviamente, si ya tenía alguna versión previa de FrontPage) o bien la de instalar el programa. La diferencia entre ambas posibilidades consiste en que mediante la primera no hay posibilidad de vuelta atrás, y todas las versiones previas del producto serán desinstaladas. Con la segunda, el usuario tiene la posibilidad de mantener ambas versiones, con el fin de trabajar indistintamente con cualquiera de ellas y comprobar las diferencias.





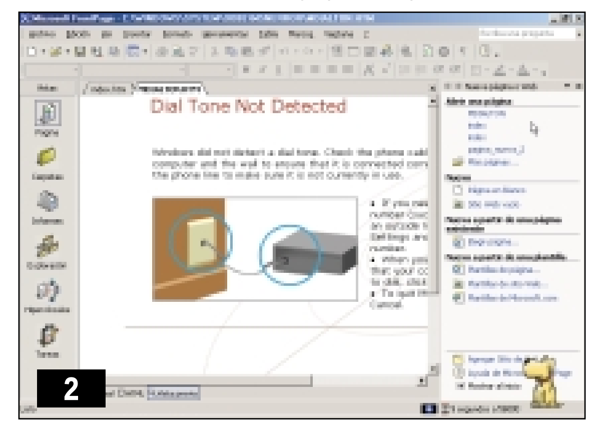
Con independencia del tipo de instalación que escojamos, FrontPage 2002 (al igual que cualquiera de las restantes aplicaciones de Office XP) sólo se podrá ejecutar libremente durante 50 veces, a menos que procedamos previamente a registrar nuestra versión original de producto. Nótese que estas 50 veces son acumulativas, dado que si instalamos Office XP conjuntamente con FrontPage 2002, y a continuación abrimos un documento de Word y una hoja Excel, cuando abramos FrontPage habremos perdido dos de las 50 veces.

2 El *Panel de tareas*

Básico

Nada más comenzar a trabajar con FrontPage, la primera novedad que salta a la vista es el denominado *Panel de tareas*, una especie de resumen breve de opciones de menú, en el que se recogen algunas de las operaciones más habituales al trabajar con la aplicación.

Para hacer uso de esta nueva utilidad, basta con pulsar sobre la opción de menú *Ver*, seleccionando a continuación la opción *Panel de tareas*. De este modo, éste se hará visible en la parte derecha de nuestra pantalla, permitiéndonos el acceso a una serie de operaciones de uso habitual. En la parte superior del mencionado panel se observan dos flechas de navegación, así como el título del conjunto de opciones visibles en ese momento. Este se puede cambiar haciendo uso del pequeño desplegable situado en la parte derecha, gracias al cual se harán visibles los 8 grupos de opciones existentes.



Una vez que hayamos abierto más de uno de dichos grupos, las flechas de navegación nos permitirán desplazarnos de unos a otros (aunque en la práctica siempre resultará más rápido hacer uso del desplegable mencionado y acceder directamente a la opción deseada).

3 Crear o abrir una página web

Básico

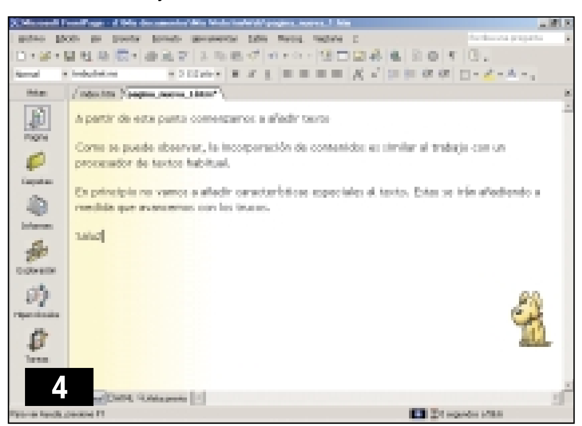
En el caso de una nueva página web, el primer paso que tenemos que llevar a cabo consiste en crearla. Para ello, si el *Panel de tareas* se encuentra visible, accederemos a la sección correspondiente a *Abrir una página* y desde allí procederemos

a generarla. Aquí son tres los grupos de opciones posibles. El primero de ellos, *Nuevo*, ofrece dos páginas web básicas pregeneradas. El segundo, *Nuevo a partir de una página existente*, toma dicho documento y genera una copia del mismo, con el fin de que lo modifiquemos en lo que sea necesario. Del tercer grupo de opciones hablaremos en el siguiente truco.
Por el contrario, si el mencionado panel no se encuentra activo, accederemos a la opción de menú *Archivo*, y seleccionaremos la opción *Nuevo*, la cual se encargará de mostrarnos dicho panel, a partir del cual procederemos como se indica en el párrafo anterior. Otra posibilidad aún más rápida consiste en pulsar sobre el icono correspondiente a la hoja en blanco (el situado más a la izquierda), con lo cual se nos creará un documento básico.
Finalmente, si el documento ya existe, son varias las opciones que tenemos para abrirlo. La primera de ellas es a partir del propio sistema operativo, pulsando sobre el botón de *Inicio* y a continuación sobre la opción *Documentos*, desde donde se muestran los documentos más recientes que hayamos abierto en el sistema.
El inconveniente de dicha opción es que se muestran todos los documentos abiertos recientemente, con independencia del tipo de éstos. Por ello, dentro de FrontPage podemos pulsar sobre la opción de menú *Archivo* y acceder a la lista de documentos recientes, situada en la parte inferior de dicha opción. Por defecto, dicha lista muestra tan sólo cuatro documentos (más adelante veremos cómo modificar dicha característica), por lo que si éste no es nuestro caso, pulsaremos sobre la opción *Abrir*, lo que nos permitirá acceder a una ventana de búsqueda. A estas dos últimas opciones se puede acceder asimismo desde el ya conocido *Panel de tareas*.

4 Escritura y formato del texto

Básico

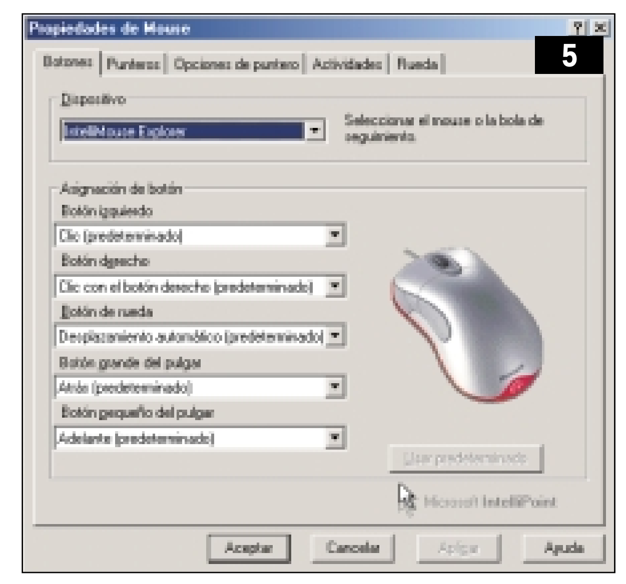
Una vez que hemos creado una nueva página web, el siguiente paso lógico consiste en dotarla de contenido. Para ello, FrontPage nos mostrará un cursor intermitente situado en la esquina superior izquierda, punto a partir del cual podremos comenzar a añadir contenido. Ese es el atractivo de los editores HTML de tipo WYSIWYG (*what you see is what you get*, lo que ves es lo que obtienes), ya que aíslan al usuario de la complejidad inherente al trabajo con *tags* o etiquetas HTML.
De esta forma, un usuario de tipo medio podría llegar a crear una página web (o incluso un sitio completo) sin necesidad de conocer nada acerca de lenguaje HTML. Por el momento, nos basta con saber que podemos ir añadiendo tanto texto como queramos, aunque en trucos posteriores aprenderemos a introducir elementos más atractivos para mejorar el aspecto de nuestro trabajo.



5 En compañía del IntelliMouse

Básico

IntelliMouse es el ratón de ergonómico y atractivo diseño que se entrega en la caja de Office XP y que nos acompañará a lo largo de nuestro recorrido por FrontPage 2002. Además de su precisión y comodidad de manejo, dicho dispositivo presenta otras dos interesantes características: por un lado, se trata de un ratón de tipo óptico (es decir, no utiliza la habitual bola de desplazamiento, sino que se posiciona por medio de láser) y, por otro, cuenta con 4 botones y una rueda, lo que le permite ofrecer funciones adicionales.

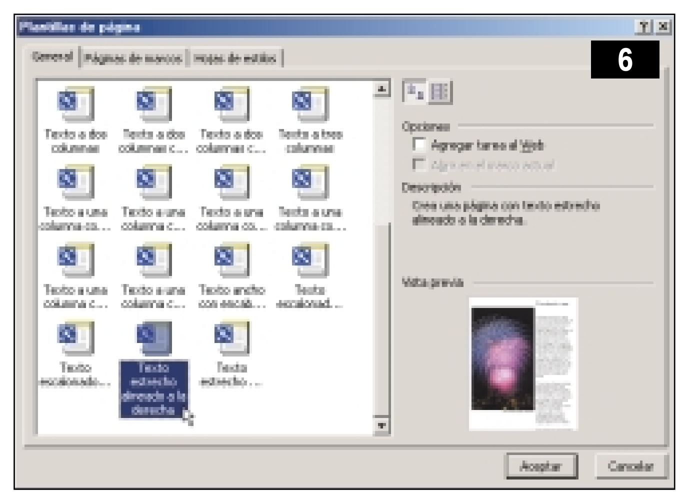


Por defecto, los botones superiores (izquierdo y derecho) cumplen las mismas funciones que en cualquier otro ratón convencional, mientras que la rueda realiza funciones similares a las de otros modelos existentes en el mercado (es decir, cuando navegamos por una página web o nos encontramos en un documento, el girar la rueda adelante y atrás nos permite desplazarnos arriba y abajo respectivamente). Por último, los dos botones adicionales situados en la parte izquierda del dispositivo sirven para efectuar las funciones de adelante y atrás (página siguiente y página anterior) cuando navegamos.
No obstante, dentro de la caja de Office XP se proporciona asimismo un CD-ROM que incluye el software necesario para poder configurar a nuestro gusto el IntelliMouse. Una vez instalado dicho software, aparecerá en la parte inferior derecha de nuestra pantalla un iconito, mediante el que podremos acceder (tras pulsar dos veces sobre el mismo) a las distintas posibilidades de configuración que se nos ofrecen, como son la asignación de funciones a cada uno de los botones o la rueda, las opciones de visualización del icono del puntero, las propias opciones del dispositivo (velocidad, visibilidad, posición, etc.) o las opciones de la rueda (desplazamiento correspondiente por cada giro, por ejemplo).

6 Plantillas mágicas

Básico

Al igual que lo que ocurre en otras aplicaciones del propio MS Office, las plantillas son documentos preformateados, dotados con una serie de características especiales con el fin de ahorrar tiempo al usuario a la hora de generar un documento de dicho tipo. Por defecto, FrontPage ofrece un buen conjunto de



plantillas predefinidas, así como asistentes capaces de generar una página nueva en función de la respuesta que proporcione el usuario frente a un conjunto de preguntas concretas. Estos asistentes son realmente potentes, y aunque sea necesario retocar en mayor o menor medida las páginas así generadas, lo cierto es que permiten ahorrar una buena cantidad de tiempo a la hora de crear la base para diseñar páginas de una cierta complejidad.

Para tener acceso a las distintas plantillas disponibles, basta con acceder a la opción de menú *Archivo*, y dentro de ésta a la opción *Nuevo* (atención, porque en el caso de las plantillas no es válido pulsar directamente sobre el icono).

Por último, un aspecto interesante: si nosotros mismos nos diseñamos nuestra propia plantilla (por ejemplo, incorporando el logo y dirección de la empresa), tenemos la posibilidad de guardar ésta para reutilizarla posteriormente. Así, desde la opción de menú *Archivo* seleccionaremos *Guardar como*, escogiendo en el cuadro que aparecerá a continuación *Plantilla de FrontPage* en el apartado correspondiente a *Guardar como tipo*.

7 Opciones perdidas

Básico

Siguiendo la misma tendencia de otros productos de Microsoft, de cuando en cuando Office XP nos «esconde» algunas opciones de menú (en realidad, lo que hace es mostrarnos los denominados *Menús abreviados*). En estos casos, para ver todas las opciones disponibles, pulsamos sobre el iconito en forma de doble flecha que aparece en la parte inferior de cada uno de estos menús. Algo similar a lo que sucede en las barras de herramientas, en la que la doble flecha se sitúa en la parte derecha de cada una de éstas.

8 Los asistentes de ayuda

Básico

En toda aplicación que se precie, la ayuda en línea juega un papel muy importante, tanto más cuanto mayor sea el número de características y opciones que esconda la mencionada aplicación.

Microsoft ha sido desde siempre sumamente consciente de dicha necesidad, dado el tipo de público al que se dirigen sus aplicaciones y las características propias de éstas. Así la ayuda en línea siempre se ha considerado como una función prioritaria dentro de sus productos, incluso con la dificultad añadida que supone el hecho de tener que trabajar con el denominado «español universal». Una vez invocada cualquiera de las aplicaciones de Office XP, se puede acceder a la ayuda en línea disponible, pulsando sobre la opción de menú identificada con un signo de interrogación. Entre las distintas opciones que aparecen en el menú desplegable que se muestra a partir de la opción mencionada, tenemos una denominada *Mostrar Ayudante de Office* (u *Ocultar el Ayudante de Office*, en caso de que éste se encuentre a la vista), que nos permitirá hacer visible la caricatura correspondiente que en ese momento se encuentre activa.

Por defecto, al instalar Office XP se define de forma automática una especie de clip como el ayudante en cuestión. Sin embargo, en cualquier momento el usuario puede seleccionar cualquier otro ayudante que le resulte más simpático, simplemente posicionando el puntero del ratón sobre el ayudante activo y pulsando el botón derecho del ratón, para finalmente escoger la opción *Elegir ayudante*.

9 ¿Dónde está el cursor?

Básico

Se ha incorporado una característica visual sumamente atractiva y eficaz, que consiste en remarcar mediante un pequeño cuadrito sombreado aquella opción de menú o icono sobre los que se encuentre situado el cursor. Gracias a ello, se acabó para siempre perder de vista la posición del cursor y mover frenéticamente éste para localizarlo mientras trabajamos con cualquiera de las aplicaciones que integran MS Office XP.

10 Barras de herramientas

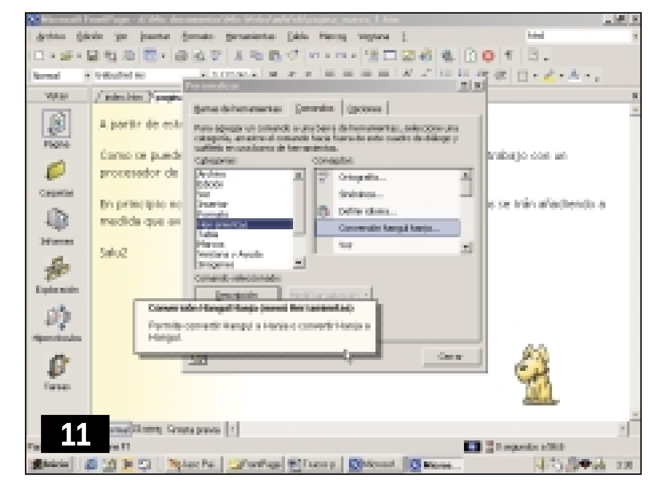
Básico

Las Barras de herramientas son conjuntos de iconos que se sitúan por debajo de la barra de menús, y que representan tareas especializadas y agrupadas mediante un cierto criterio de similitud. Así, tenemos barras de formato, de imágenes, de estilo, de lienzo de dibujo, de efectos DHTML, etc. Para hacer visible cualquiera de ellas, accederemos a la opción de menú *Ver*, seleccionaremos *Barras de herramientas*, y allí marcaremos aquella o aquellas que nos interese visualizar.

11 Modificar Barras de herramientas

Básico

Aunque las Barras de herramientas que se entregan por defecto incluyen un buen número de opciones, suficientes en la



mayoría de los casos para satisfacer las necesidades más habituales, es posible que para algunos usuarios éstas se queden cortas. Para solucionar este «inconveniente» podemos acceder de nuevo a la opción de menú *Ver*, y dentro de ésta a *Barras de herramientas*, seleccionando la opción *Personalizar* y accediendo en este caso a la pestaña central, *Comandos*. Desde aquí podremos seleccionar la Barra de herramientas que queremos modificar y añadirle cuantas opciones consideremos oportunas.

12 Crear una nueva Barra de herramientas

Básico

Incluso con lo que hemos visto en el truco anterior, habrá quien opine que esto no es suficiente (sobre gustos, no hay nada escrito). Sin embargo, en Microsoft ya se había previsto esta necesidad y, de la misma forma que se puede modificar una Barra de herramientas concreta para adaptarla a nuestras necesidades, nada impide que podamos crear nuestra propia barra personalizada.

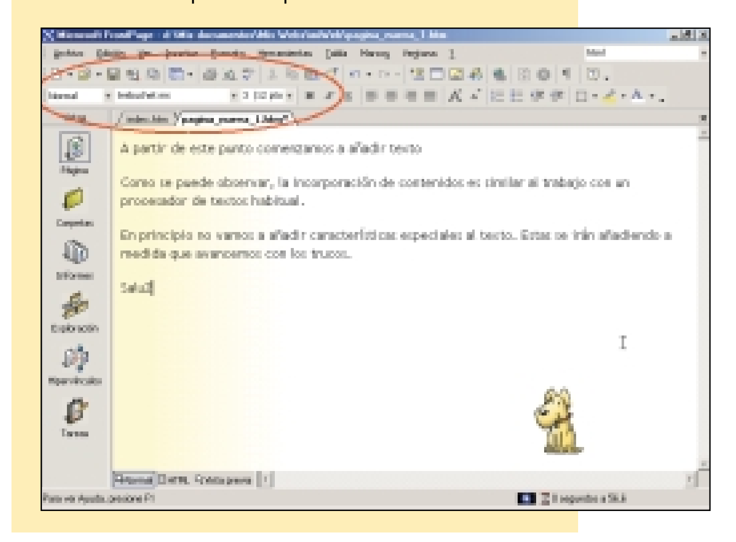
El procedimiento es sencillo: nos dirigiremos a la opción de menú *Ver*, y dentro de ésta escogeremos sucesivamente las opciones correspondientes a *Barras de herramientas* y *Personalizar*, accediendo por último a la pestaña etiquetada *Barras de herramientas*. En esta ventana existe un botón etiquetado *Nueva*, que es con el que crearemos la barra en cuestión. A dicha barra tendremos que darle también un nombre y especificar si será visible para todas las páginas creadas a partir de ese momento.

13 Seleccionar la fuente

Básico

Cuando comenzamos a escribir en FrontPage, lo habitual es que empecemos haciendo uso de un estilo normal con sus características definidas por defecto (es decir, un tipo de letra, con un cierto tamaño e incluso unos algunos atributos).

Si tenemos activa la *Barra de herramientas Formato*, cambiar el tipo de letra es tan sencillo como desplegar el segundo cuadro (el primero corresponde a los estilos) y seleccionar allí el tipo que nos interese. Si marcamos una palabra o párrafo, el nuevo tipo de letra se aplicará tan sólo a dicha palabra o párrafo.



14 Atributos básicos

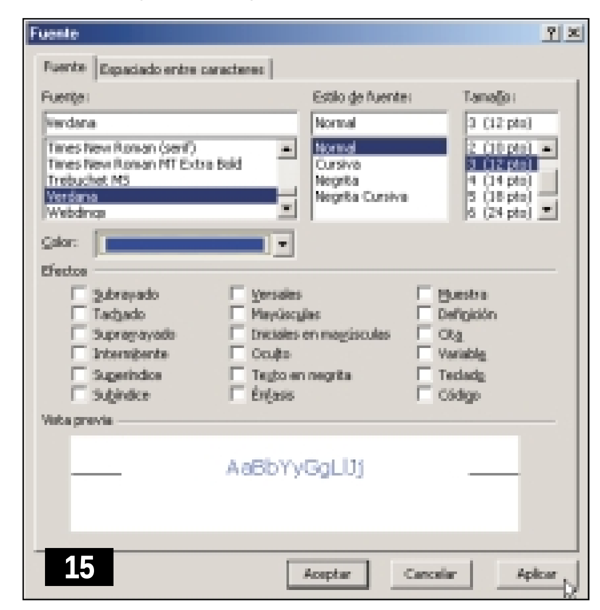
Básico

Continuando con la mencionada *Barra de herramientas*, al lado del desplegable anterior nos encontramos con otro que tan sólo muestra números. Se trata del tamaño en puntos, y hay que tener muy presente que tipos de letra distintos con un mismo tamaño en puntos presentan alturas (tamaños) distintas. Jugar con el tamaño de los caracteres puede ayudarnos a resaltar o enfatizar algunas palabras, pero lo habitual será que hagamos uso de ciertos atributos básicos, como son la negrita, la cursiva y el subrayado. Todos ellos se encuentran situados justo a la derecha del desplegable correspondiente al tamaño de la fuente.

15 El formato de fuente

Básico

Aunque en trucos anteriores ya hemos visto cómo seleccionar el tipo y tamaño de fuente, así como aplicar ciertos atributos básicos, lo cierto es que FrontPage nos ofrece más posibilidades de configuración respecto al formato de fuente.



En efecto, para hacer uso de las mismas, basta con acceder a la opción de menú *Formato*, y dentro de ésta escoger la opción correspondiente a *Fuente*. Aparecerá entonces un nuevo formulario que consta de dos pestañas: en la primera podremos seleccionar todas las características que queremos aplicar al texto, como pueden ser el tipo de fuente, su estilo y su tamaño, su color, el estilo de subrayado y el color de éste, y otros efectos especiales.

Para comprobar el aspecto final de nuestra selección de características, en la parte inferior de dicho cuadro se muestra una pequeña ventanita de vista previa.

16 El formato de párrafo

Básico

Análogamente a lo que sucede en el caso del formato de fuente, FrontPage 2002 también nos permite especificar las distintas características que queremos aplicar a cada párrafo. Entre éstas podemos citar el tipo de justificación (alineado a la

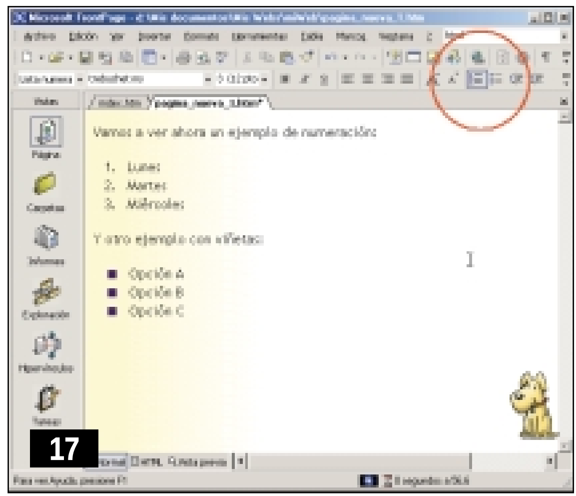
izquierda, alineado a la derecha, centrado o justificado), el espacio anterior o posterior con otros párrafos, o la sangría (es decir, el posible endentado de la primera línea).

17 Numeración y viñetas

Básico

Estos son dos recursos habituales cuando se trata de hacer una enumeración de puntos o elementos, en especial el segundo, puesto que el primero lleva implícito además un matiz de orden o importancia.

Para hacer uso de ambos recursos, basta con acceder a sendos iconos que aparecen en la *Barra de herramientas Formato*, uno con los números 1, 2 y 3, y otro con tres puntos alineados verticalmente, al lado de los cuales aparecen unas rayas horizontales. De hecho, la forma habitual consiste en seleccionar el texto que queremos presentar en ese formato, y pulsar a continuación uno de estos iconos.



Ahora bien, si no nos gusta el formato que aparezca, podemos seleccionar de nuevo dicho texto y acceder a la opción de menú *Formato*, en la opción correspondiente a *Numeración y viñetas*, de modo que podamos escoger la forma que más nos guste. Esto se puede conseguir también seleccionando el texto, posicionando el cursor encima de éste y pulsando el botón derecho del ratón.

18 *Vista previa en el navegador*

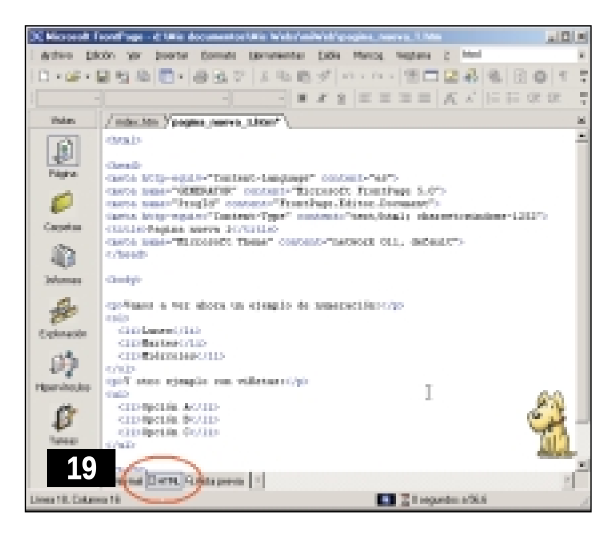
Básico

Para comprobar el estado final de nuestro página web cuando la visualicemos a través de un navegador HTML o, simplemente, para comprobar cómo evoluciona a medida que la vayamos diseñando, FrontPage nos ofrece la característica de *Vista previa en el navegador*. Para acceder a la misma, pulsaremos sobre la pestaña situada en la parte inferior, junto a las pestañas de normal y HTML, o bien accederemos a ésta desde la opción de menú *Archivo*.

19 Vista del código HTML

Básico

De forma análoga, y aunque generalmente no será necesario a la hora de diseñar nuestras páginas web, en algunas ocasiones puede resultarnos útil echar un vistazo al código HTML subyacente. Obviamente, esta opción sólo será de interés en aquellos

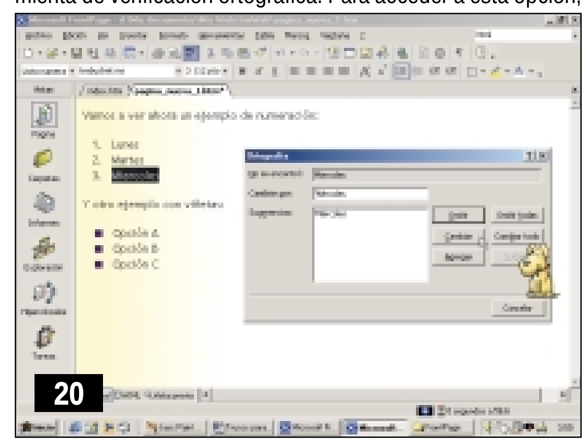


casos en los que tengamos conocimientos necesarios acerca de dicho lenguaje y exista algún tipo de problema que justifique su resolución a dicho nivel. En caso contrario, lo mejor es no tocar el código, puesto que la modificación de alguna de las etiquetas puede conducir a la obtención de efectos inesperados. La visualización del código HTML se consigue simplemente pulsando sobre la pestaña situada en la parte inferior, que se encuentra etiquetada con la palabra *HTML*.

20 Verificar la ortografía

Básico

Una de las herramientas con carácter propio en toda aplicación que maneje texto (e indudablemente un editor HTML entra dentro de esta categoría) y que se precie es su herramienta de verificación ortográfica. Para acceder a esta opción,



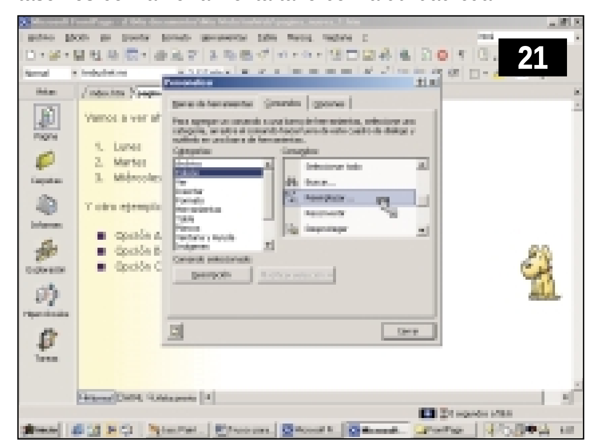
podemos pulsar sobre el icono de la *Barra de herramientas Estándar* que muestra las letras a, b y c sobre una marca de comprobación, acceder a la opción de menú *Herramientas* y seleccionar allí *Ortografía*, o, lo más rápido y recomendable, pulsar la tecla «F7» en cualquier punto del documento que queramos verificar.

21 Agregar o quitar botones

Básico

Anteriormente ya hemos mencionado la importancia que poseen en FrontPage las barras de herramientas y hemos visto los distintos tipos que existen. Sin embargo, en la prác-

tica esto no siempre es suficiente, puesto que a la hora de trabajar con una barra de herramientas concreta podemos echar en falta una determinada función, o bien considerar que podríamos llevar a cabo algún proceso de forma más eficaz si contásemos con la herramienta tal o con la utilidad cual.

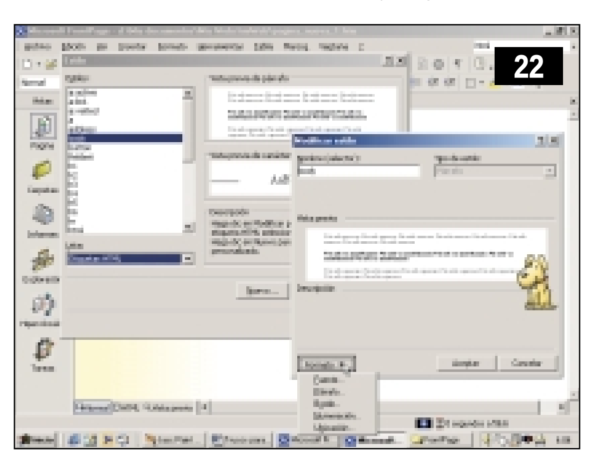


Por fortuna, este proceso ha sido tenido en cuenta en el diseño de FrontPage (no es algo exclusivo de la versión 2002), de modo que si necesitamos añadir nuevos botones a cualquier barra de herramientas el procedimiento es relativamente simple. Para ello tenemos que tener visible la barra de herramientas que pretendemos ampliar. Seguidamente accederemos a la opción de menú *Ver*, escogiendo a continuación *Barras de herramientas* y, por último, seleccionando la opción *Personalizar*. De las tres pestañas disponibles tenemos que activar la central, *Comandos*. Ahora tenemos que localizar entre los dos paneles de la pestaña mencionada el comando que queremos añadir a la barra de herramientas en cuestión. El último paso consiste en posicionar el cursor sobre dicho comando y, sin soltar el botón izquierdo del ratón, «arrastrarlo» hasta situarlo encima de la barra de herramientas, soltando entonces el mencionado botón.

22 Estilos y formato

Básico

Los estilos son una de las características distintivas de Microsoft FrontPage, hasta el punto de que el usuario que maneja el programa pero no ha hecho uso jamás de los estilos, no llega a aprovechar ni la cuarta parte de las posibilidades que la aplicación le brinda. Dicho así, puede parecer un tanto chocante, pero si tenemos en cuenta que un estilo es un conjunto de características concretas de un texto (un tipo determinado,



con un tamaño determinado y unas características determinadas) asignado a una función concreta (título de primer nivel, título de segundo nivel, etc.), entonces podemos comenzar a intuir el abanico de oportunidades que los estilos nos brindan. A modo de ejemplo, una vez fijadas las características de un Encabezado 1, las siguientes líneas de texto que utilicen el mismo estilo presentarán también el mismo aspecto. Análogamente, si sobre la marcha decidimos cambiar las características de dicho estilo, bastará con aplicarlo de nuevo a todo el documento, para que de inmediato todas las líneas que hacen uso de dicho estilo queden actualizadas, sin necesidad de ir una por una.
Para aplicar un estilo a un texto concreto, bastará con seleccionarlo y escoger a continuación el estilo que se le quiere aplicar, pulsando en la *Barra de herramientas Formato* sobre el primer desplegable que se encuentra en la parte de la izquierda. El mismo resultado se puede conseguir también a partir de una opción de menú o pulsando sobre el primer icono por la izquierda, el de las dos Aes en paralelo (aunque el proceso será más lento).

23 Personalizar un estilo

Básico

Una vez que se comienza a trabajar con estilos, el siguiente paso lógico consiste en modificar el aspecto de los ya existentes y en crear otros nuevos, más adaptados a nuestras propias necesidades. Como punto de partida inicial, accederemos a la opción de menú *Formato* y seleccionaremos la opción correspondiente a *Estilo*, en la que se nos muestran todos los estilos existentes en la plantilla con la que se haya creado la página con la que estemos trabajando.
Para modificar un estilo ya existente, el siguiente paso consiste en marcarlo con el cursor y pulsar el botón *Modificar*. Aparecerá entonces una nueva ventana, con las características del estilo seleccionado, en la que pulsaremos sobre el botón *Formato* para seleccionar qué queremos cambiar.

24 Aplicar un tema

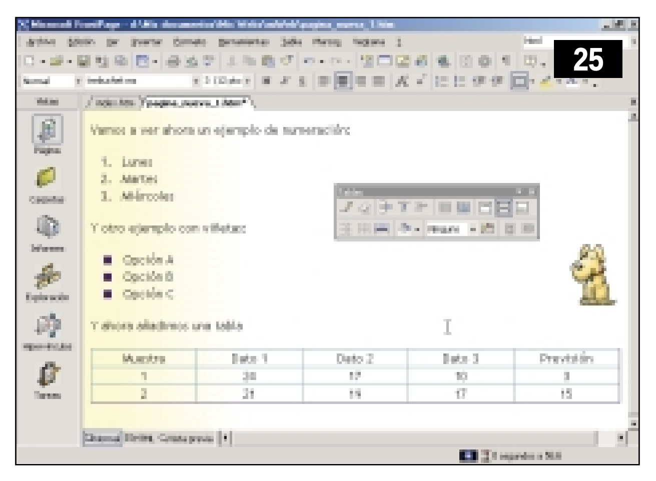
Básico



Una vez concluida la generación y elaboración de los contenidos de una página, podemos ir un paso más allá y modificar su aspecto general mediante la aplicación de un tema, es decir, un esquema visual prediseñado que aplica un aspecto coherente a todos los elementos de la misma. Accedemos a la opción *Tema* dentro del menú *Formato*. A partir de aquí, el usuario tan sólo necesita escoger el tema y las características asociadas, y aplicarlo. De este modo, se afectará a elementos tales como el tipo de letra (incluyendo tamaño y color), el fondo de página, los elementos de división horizontal, el formato de las viñetas, los colores de los hipervínculos o los colores de los bordes de las tablas.

25 Creación y manejo de tablas

Básico



Es de sobra conocido que las tablas son una estructura que permite organizar la información de forma muy clara. De ahí que sean tan utilizadas en cualquier tipo de documentos, puesto que ayudan a resumir información que de otra forma ocuparía bastante espacio.
Buena prueba de la importancia de este tipo de estructura organizativa lo constituye el hecho de que en FrontPage existe una opción de menú, con todas sus subopciones asociadas, dedicada en exclusiva a las tablas. De este modo se permite añadir y eliminar filas, columnas y celdas de forma muy sencilla. Para insertar una tabla en nuestro documento podemos hacerlo a través de dicha opción de menú, o bien de forma más rápida a partir del icono de tabla que aparece en la *Barra de herramientas Estándar*, siendo necesario en este último caso únicamente marcar el número de filas y casillas que queremos incluir.

26 De texto a tabla, y viceversa

Básico

La integración de las funciones de tabla con FrontPage va aún un poco más allá, ya que la propia aplicación incorpora dos pequeñas utilidades que permiten que, dado un texto concreto, con separaciones concretas entre elementos, lo transformemos en una tabla. Y análogamente, que a partir de una tabla se genere texto puro. A ambas opciones se accede a través de las respectivas subopciones del apartado de menú *Convertir*, dentro de *Tabla*.

27 Dar formato a una tabla

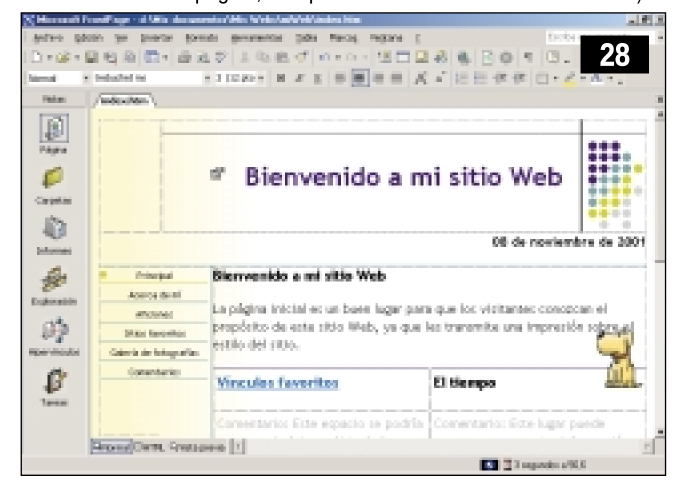
Intermedio

Como hemos visto previamente, crear una tabla es sencillo... pero no es vistoso, dado que ésta se crea con las opciones por defecto. Esto nos servirá como tal en la mayoría de los casos, pero habrá ocasiones especiales en las que haya que cuidar un poquito más esa presentación.
La respuesta a este problema se denomina *Autoformato de tablas*, a la que se accede desde la opción de menú *Tablas*. Tras invocar a esta herramienta, nos aparecerán todos los formatos de tabla predefinidos que FrontPage nos puede ofrecer, pero además tenemos la posibilidad de personalizar estos formatos sin más que seleccionar uno cualquiera de ellos y pulsar sobre el botón *Modificar*.

28 Las vistas de FrontPage 2002

Básico

La columna de vistas sirve para gestionar el manejo con páginas y sitios web. Cada vista es una forma o modo especial de representación de un aspecto distinto de la información contenida en un sitio web (en el caso más simple, podemos hacer la equivalencia de que una página individual es un sitio web de una única página, aunque esto no sea estrictamente cierto).

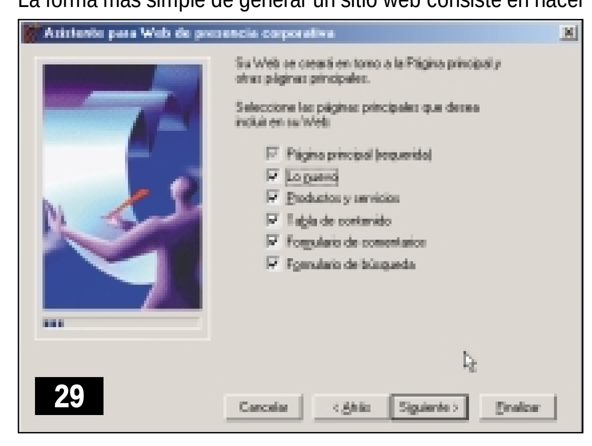


La vista de página es la primera de las vistas posibles, y posiblemente una de las que utilizaremos con mayor asiduidad a la hora de trabajar con FrontPage, dado que su cometido es precisamente ese: el de servirnos para modificar las características o contenidos de una página HTML concreta.
Esta vista consta en realidad de tres vistas posibles, según ya hemos comentado previamente, haciendo uso de las pestañas situadas en la parte inferior: *Normal*, *Html* y *Vista previa en el navegador*. En este sentido cabe destacar que, en la vista *Normal,* podemos encontrarnos con que algunos elementos no se muestran correctamente, o bien se muestran como objetos insertados.

29 Creación de sitios web

Básico

Antes de continuar con la descripción detallada de las vistas restantes, vamos a hacer un breve inciso para mencionar cómo crear un sitio web, ya que las otras vistas que FrontPage nos ofrece sólo tienen sentido si estamos hablando no ya de una página individual, sino de un sitio web completo.
La forma más simple de generar un sitio web consiste en hacer



uso de alguna de las plantillas disponibles o, preferiblemente, de alguno de los asistentes que se encargarán, de acuerdo con las preferencias que les indiquemos, de organizar la estructura completa del sitio así como las páginas necesarias.
Posteriormente, podremos añadir nuevas páginas y tendremos que encargarnos de modificar los contenidos de las ya creadas, puesto que éstos se basan en plantillas y, como es de suponer, no aportan información válida.
Para acceder a estas plantillas o asistentes, la forma más rápida consiste en seleccionar la opción *Nuevo* en el menú *Archivo*, a continuación *Página o Web*, y cuando se visualice el *Panel de tareas* escoger la opción *Plantillas de sitio Web...*.

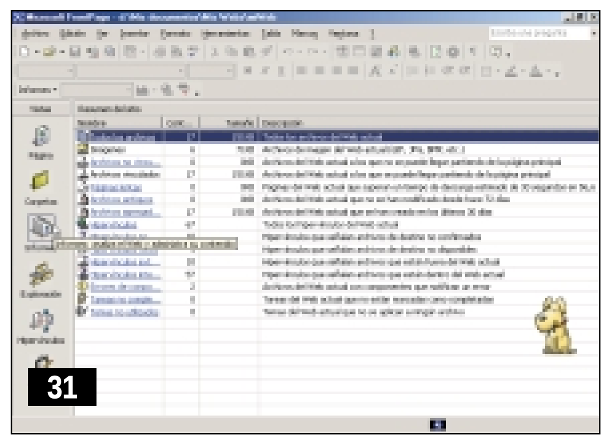
30 La vista de carpetas

Básico

Similar al *Explorador* de Windows, esta vista permite organizar nuestra web en carpetas y subcarpetas, simplificando así las tareas de organización de archivos y movimiento de información. Se trata de una vista especialmente diseñada para mantener la estructura del web, de modo que, cuando trasladamos un archivo de carpeta, por ejemplo, se encarga de actualizar todos los enlaces existentes hacia o desde dicho archivo.

31 La vista de informes

Básico



Posiblemente una de las vistas más útiles, cuya aparición tuvo lugar en la versión previa de FrontPage. Nos proporciona una visión global y detallada de todos los componentes y eventos que contiene nuestro sitio web, como número de páginas, número de hiperenlaces, etc. Sin embargo, la información realmente útil es la que hace referencia a los posibles errores que pueda contener el sitio, como pueden ser eventos erróneos, hipervínculos que no conducen a ninguna parte, componentes que no funcionan de la forma esperada, etc.
Además, si hacemos doble clic sobre cualquiera de las líneas del informe, obtendremos una información más detallada acerca del evento reflejado en dicha línea.

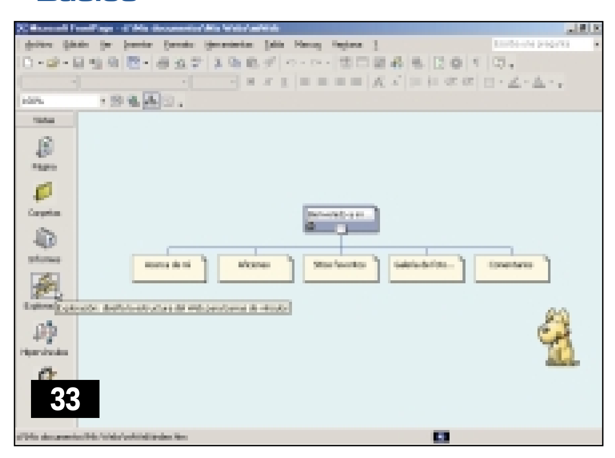
32 La vista de exploración

Básico

Esta estructura nos permite tener una vista jerárquica de la organización de nuestro sitio web, en forma de diagrama. Existe una página cabecera (denominada normalmente «index.htm»), a partir de la cual se ramifican otros niveles. Su principal utilidad consiste en que permite añadir nuevas páginas a determinados niveles de la estructura, lo que posteriormente será de utilidad a la hora de gestionar tablas de contenidos (es decir, conjuntos de enlaces que se generan automáticamente basándose en dicha jerarquía).

33 La vista de tareas

Básico

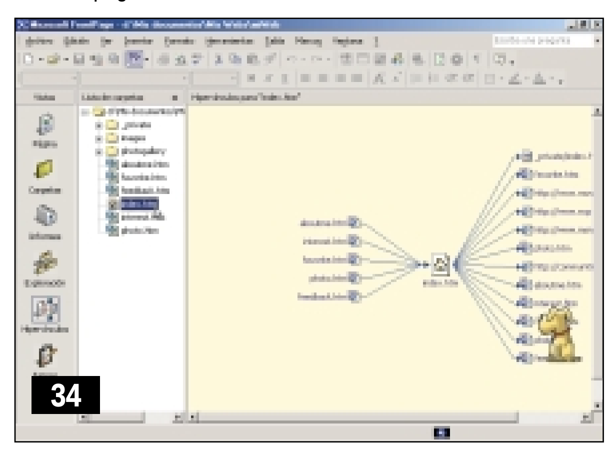


Si somos un poquito «despistados» o, simplemente, nos gusta tener las cosas bien organizadas, la vista de tareas puede convertirse en una gran aliada a la hora de construir nuestro sitio web. Su misión no es otra que la de permitirnos apuntar todas las cosas que están pendientes de hacer, como una especie de recordatorio por si no podemos resolverlas en el mismo momento.

34 La vista de hipervínculos

Básico

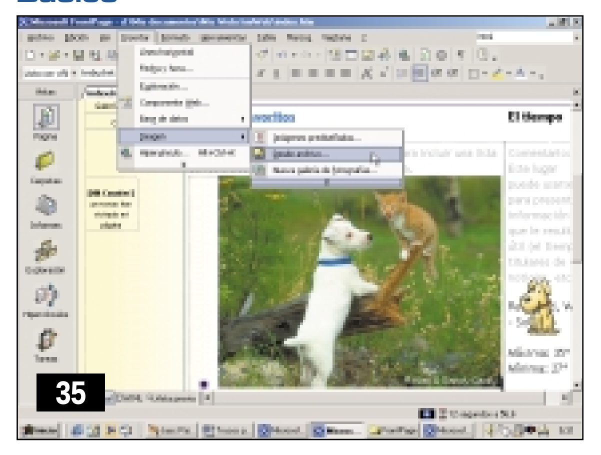
Esta vista se puede definir en buena medida como complementaria de la vista de exploración. En efecto, su cometido es muy sencillo, puesto que lo que nos permite es conocer rápidamente la estructura de hiperenlaces existente entre las distintas páginas.



Sin embargo, la primera vez que accedamos a dicha vista observaremos que aparentemente no existe la posibilidad de seleccionar las páginas cuyos enlaces queramos comprobar. Pues bien, ése es el motivo por el que decíamos que esta vista es complementaria de la vista de exploración: es preciso acudir a esta última, seleccionar la página cuyos enlaces queremos estudiar, y volver de nuevo a la vista de hipervínculos.

35 Inserción de hipervínculos

Básico



Y ya que hemos hablado de los hipervínculos o hiperenlaces, no estaría de más que explicásemos cómo hacer uso de los mismos en nuestras propias páginas. Los hiperenlaces son la esencia de la Web, puesto que son el mecanismo fundamental para enlazar información. En esencia, no son más que eso: enlaces a direcciones URL en las que se encuentran almacenados los elementos referenciados. Dichas URL pueden ser ficheros que están en la propia web, direcciones remotas, otras partes dentro de la propia página html desde la que se efectuará el salto o incluso otros tipos de información, como una dirección de correo electrónico, por ejemplo.
Para insertar un hiperenlace en una de nuestras páginas, basta con seleccionar el texto o imagen que queremos que sirva como activador del salto, y acceder a continuación a la opción de menú *Insertar*, seleccionando entonces la opción *Hipervínculo*. Se desplegará entonces una ventana emergente, en la que tendremos que escoger el tipo de hiperenlace que queremos utilizar, así como la dirección de destino.

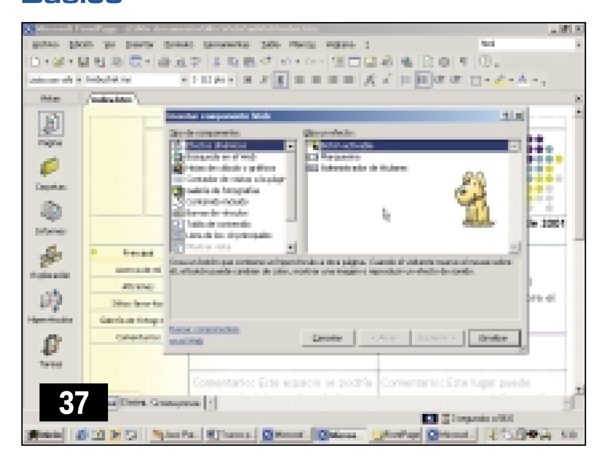
36 Inserción de imágenes

Intermedio

La operación de añadir imágenes a nuestras páginas web es realmente sencilla, incluso más que en el caso de los hiperenlaces. En este caso, bastará con acceder a la opción de menú *Insertar* y escoger la opción *Imagen*. Se desplegará entonces un nuevo menú con distintas opciones, de las que tendremos que seleccionar aquella que más se adapte a lo que necesitamos. En general, si lo que queremos es insertar una imagen que está en un archivo, haremos uso de la opción *Desde archivo*, indicando a continuación la ubicación física de dicho archivo. La opción de imágenes prediseñadas corresponde a una galería de imágenes que Microsoft proporciona junto con la aplicación, aunque también cabe la posibilidad de acceder a la Web para descargar imágenes adicionales si ninguna de las que se nos han facilitado cumple con lo que estamos buscando.

37 Inserción de componentes

Básico



También dentro de la opción de menú *Insertar* podemos tener acceso a otros componentes, que permitirán dotar a nuestras páginas de distintos atractivos. Son los denominados componentes activos, aunque en esta versión de FrontPage aparecen etiquetados como *Componentes Web*. De hecho, es probable que los usuarios de versiones anteriores de FrontPage echen en falta la disponibilidad de tales elementos a un primer nivel, como podían ser las marquesinas, los botones activables, etc., pero lo que no debemos perder de vista es que con la versión 2002, la cantidad de elementos disponibles de este tipo ha aumentado de forma sensible, lo que ha provocado a su vez la necesidad de organizarlos de manera adecuada. En concreto, junto a los elementos indicados, aquí también podemos encontrar los elementos de hoja de cálculo y base de datos, así como la posibilidad de incorporar código Java o controles ActiveX.



McAfee Internet Security 4.0

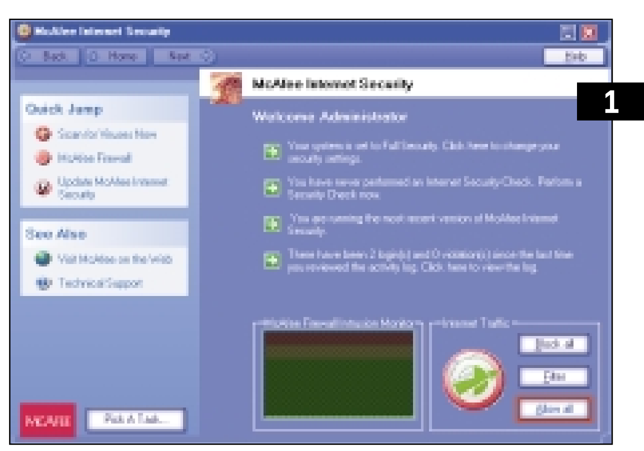
Protege tu equipo de las amenazas que pueblan la Red / CD

Todos los usuarios aficionados a navegar en Internet son conscientes, en mayor o menor medida, de la existencia de numerosos peligros capaces de acechar de las formas más insólitas con la finalidad de atentar contra la integridad y privacidad de los datos almacenados en sus ordenadores. Probablemente las amenazas más populares sean los virus, debido en gran medida a la labor divulgadora realizada por numerosos medios de comunicación, ajenos en principio al panorama informático. Sin embargo, a pesar del conocimiento generalizado que existe de esta amenaza real, incluso conociendo casos verídicos publicitados hasta la saciedad, es realmente frecuente comprobar que estos peligros son a menudo menospreciados por los usuarios más confiados. Esto es un error. No hay peor forma de aprender que hacerlo cuando uno ya ha padecido las consecuencias de su dejadez inicial. Esta circunstancia se vuelve aún más relevante cuando los datos que habitan en el disco duro no son simples juegos y ficheros MP3, casos en que debe prestarse especial atención a la seguridad en todo lo referente a la exploración del ciberespacio y sus consecuencias. A pesar de que en un principio puede parecer que mantener un nivel de seguridad y privacidad óptimo es complicado, nada más lejos de la realidad. No es necesario utilizar complejas aplicaciones difíciles de configurar, ni siquiera multitud de herramientas dispuestas a husmear en los más recónditos recovecos de nuestro equipo. Al igual que la informática ha evolucionado poniendo a disposición de todos los usuarios sistemas operativos y aplicaciones realmente potentes y muy sencillas de utilizar, el software encargado de mantener la salud de nuestro PC cuando lo conectamos a Internet ha hecho lo propio. Hoy en día no sólo es posible, sino realmente asequible, obtener el máximo partido de estas herramientas y afrontar nuestras incursiones en la Red con garantías. Y, precisamente, es en este ámbito donde destaca la *suite* que protagoniza este capítulo: McAfee Internet Security 4.0.

1 Seguridad, ¿por qué?

Básico

Antes de analizar cuáles son realmente las amenazas a las que cualquier usuario de la Red está expuesto, vamos a matizar cuáles son las dos premisas básicas de las que partimos cuando hablamos de seguridad en Internet: proteger la integridad de la información almacenada en la máquina y salvaguardar la privacidad de los usuarios de la potencial amenaza de pequeños, y en ocasiones no tan pequeños, programas diseñados para recopilar información privada acerca de éstos.

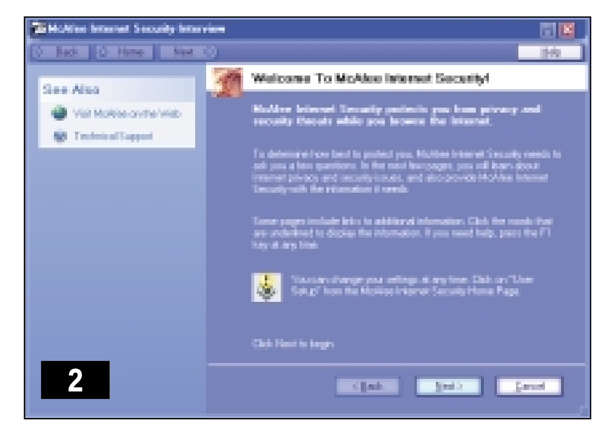


Hoy en día es habitual utilizar nuestro PC para realizar compras *on-line*, gestionar transferencias bancarias, matricularse en la universidad, etc. Como vemos, posibilidades sumamente interesantes que en todos los casos conllevan un riesgo añadido del que es posible prescindir. Por fortuna, gigantes como Microsoft y Netscape investigan constantemente con la finalidad de mejorar sus navegadores con tecnología que dificulte al máximo las dañinas acciones de los *hackers*. Un ejemplo es la adopción de la técnica de encriptado *Secure Sockets Layer* (SSL) por parte de ambos productos, lo que evidencia la necesidad de apostar por la seguridad en ambos extremos de la cadena: el del servidor y el del cliente. En efecto, no basta con que la tienda virtual en la que introducimos el número de nuestra tarjeta de crédito garantice nuestra seguridad. Es necesario que el equipo del usuario, como partícipe activo en la transacción, disponga de un mínimo de seguridad que garantice la viabilidad de ésta de forma conjunta a la seguridad estipulada por el servidor.
Como hemos comentado en la introducción del capítulo, los virus, a pesar de ser la amenaza más popular, no constituyen el único peligro que puede dañar la integridad de la información almacenada en los equipos de los usuarios. Por desgracia, la lista de posibles agentes dañinos es realmente holgada: controles ActiveX y *applets* Java capaces de llevar a cabo acciones realmente malintencionadas, programas que establecen vías de comunicación con el exterior que escapan al control del usuario, aplicaciones que acceden a información confidencial, servidores web capaces de almacenar *cookies*

cuanto menos sospechosas en los equipos de los usuarios, etc. En definitiva, una larga lista de amenazas que es posible neutralizar o, al menos, minimizar sustancialmente, a través de una herramienta tan potente y sencilla de utilizar como la que vamos a conocer en los siguientes apartados.

2 Los primeros pasos

Básico



La instalación de McAfee Internet Security es tan sencilla como puede serlo la de cualquier *suite* de carácter, por ejemplo, meramente ofimático. Una vez concluido dicho proceso y tras iniciar la herramienta (ruta *Inicio/Programas/McAfee/McAfee Internet Security*), un eficaz asistente propondrá al usuario la dedicación de unos minutos a contestar unas sencillas preguntas que permitirán a la herramienta autoconfigurarse y adoptar un perfil de seguridad de acuerdo a las preferencias y necesidades del usuario. Es necesario saber que, como es lógico y al igual que cualquier otra aplicación de monitorización de seguridad, la herramienta permanece ejecutándose en segundo plano o *background*, por lo que es recomendable que el usuario determine el equilibrio entre el nivel de seguridad que desea utilizar en su equipo y el impacto en el rendimiento que va a suponer la ejecución del módulo de monitorización. Cuanto mayores sean las exigencias de seguridad, mayor será la carga de trabajo de dicho módulo y, por tanto, en mayor medida afectará al rendimiento global del equipo. Las preguntas según las cuales dicho asistente determinará el nivel de seguridad que debe imponer al equipo permiten al usuario, por ejemplo, definir un grado de exigencias en lo que a la seguridad y privacidad se refiere entre tres posibles, o especificar qué datos deben ser especialmente tratados, como podrían ser los números asociados a las tarjetas de crédito. Una vez finalizada esta sencilla tarea de configuración, será posible realizar un análisis exhaustivo de la seguridad del equipo, lo que permitirá a la herramienta determinar los puntos débiles de la máquina y solventar las carencias asociadas a éstos.

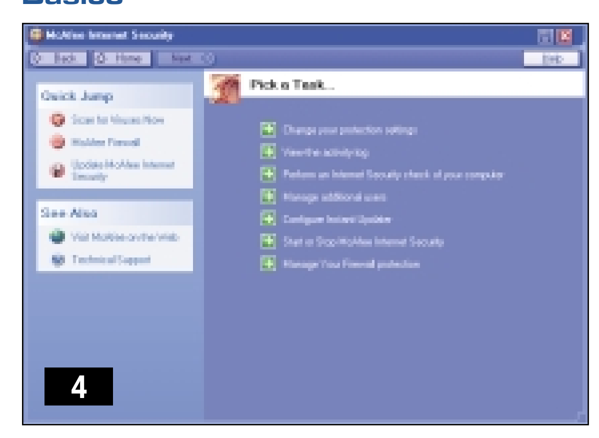
3 Su forma de trabajo

Básico

Una vez que el usuario ha completado la «entrevista» mencionada en el apartado anterior, la herramienta está en disposición de afrontar la autoconfiguración de los distintos módulos que describiremos en los siguientes apartados y, en consecuencia, podrá iniciar su labor. Para ello utiliza una utilidad denominada *McAfee Guardian*, que permanece en ejecución en segundo plano vigilando los distintos «agujeros» que podrían servir como punto de entrada al equipo de las diversas amenazas que hemos analizado previamente. Este módulo se refleja en la *Barra de tareas* de Windows en forma de un icono situado en la esquina inferior derecha junto al reloj del sistema, a través del cual es posible acceder al *Panel de control* general de la aplicación. Para ello, tan sólo es necesario utilizar el menú contextual de la utilidad (botón derecho del ratón) y seleccionar la opción *Internet Security/Run McAfee Internet Security*.
Para facilitar la utilización de la *suite* al usuario y maximizar su eficacia, de vez en cuando la herramienta solicitará la contestación de alguna pregunta adicional. Como vemos, la labor de configuración de esta magnífica aplicación de Network Associates se basa fundamentalmente en el método pregunta-respuesta, lo que va a manifestar su influencia en la interfaz de usuario, tal y como veremos en el siguiente apartado.

4 Una interfaz de lo más intuitiva

Básico

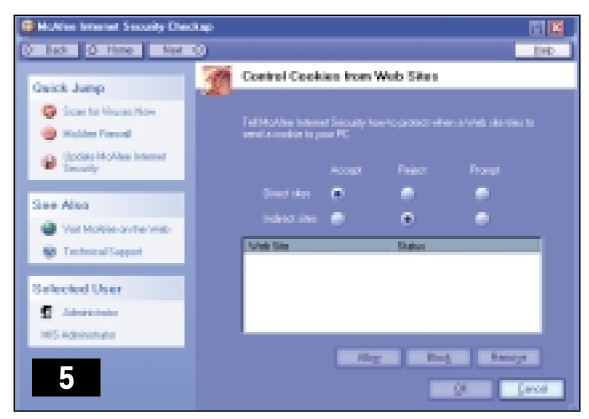


Si algo caracteriza esta aplicación de seguridad es la sencillez extrema de su interfaz. Como hemos mencionado con anterioridad, la configuración de la herramienta se fundamenta en un conjunto de preguntas que la *suite* realiza al usuario con la finalidad de conocer sus preferencias. Por este motivo, no encontraremos en la interfaz abundantes menús, complejas opciones o ininteligibles términos, nada de eso. Tan sólo veremos enlaces adosados a un texto descriptivo en el que se explica qué logrará el usuario si hace clic sobre dicho vínculo, y algunos botones que cederán el protagonismo al módulo de ayuda al usuario, al antivirus o al *firewall*, entre otros. Una gran idea que permite que prácticamente cualquier persona, por escasos que sean sus conocimientos de informática, aproveche las ventajas de la *suite* beneficiándose de una navegación segura en la Red.

5 El gestor de *cookies*

Básico

Bajo este sugerente nombre se esconden unos pequeños ficheros que son almacenados en los PC de los usuarios y enviados por los navegadores a determinados servidores web. Gracias a estos ficheros, las páginas en cuestión conocen las preferencias de los usuarios, su nombre y contraseña de acceso a dicha web, etc. Hasta ahora todo parece correcto, de hecho si su utilidad se restringiese a lo que hemos comentado hasta ahora, las *cookies* no serían susceptibles de originar problema alguno. Sin embargo, además de proporcionar la información anteriormente mencionada, cabe la posibilidad de que estos ficheros alberguen datos privados que el usuario no desea divulgar, como contraseñas de la máquina, datos bancarios o cualquier otra información que no deba ser divulgada.

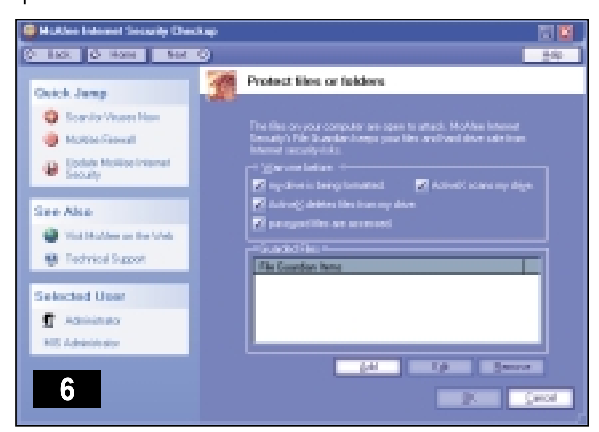


Por este motivo, es de vital importancia que exista un mecanismo que permita controlar con exactitud la utilización de las *cookies*, impidiendo a los sitios web sospechosos la creación de estos ingeniosos archivos en el equipo del usuario. Y, por supuesto, McAfee Internet Security cumple a la perfección dicha premisa. El gestor de *cookies* permite al usuario definir tres opciones básicas que le permitirán controlar la utilización de estos elementos en su equipo: bloquear todas las *cookies*, permitir su utilización y eliminarlas del equipo. Estas tres posibilidades deben definirse en función de dos tipos diferentes de conexión a páginas web: conexión directa e indirecta. La conexión directa se efectúa cuando el usuario teclea en la *Barra de direcciones* del navegador la URL de la página a la que desea conectarse, o hace clic con el ratón en un hipervínculo que le catapultará a la página a la que desea acceder. Sin embargo, la conexión indirecta se origina cuando en el navegador se descarga de forma automática una página o marco que estaba vinculado a la página a la que realmente queríamos acceder. En estos casos, las opciones al alcance de los usuarios son tres: aceptar las *cookies*, rechazarlas o tratar a cada una de ellas de forma independiente (opción *prompt*). Esta última posibilidad solicita la intervención del usuario cada vez que un servidor web envíe una *cookie* al navegador.

6 Protección de la intimidad

Básico

En la actualidad, los sistemas informáticos centralizan todos los órdenes de la vida, por lo que no es de extrañar que en el PC de cualquier usuario doméstico puedan encontrarse documentos bancarios, extractos de recibos telefónicos o cualquier otra información de evidente índole privada. Lógicamente, mantener estos datos fuera del alcance de terceros es vital. Para ilustrar esta idea utilizaremos un ejemplo: supongamos que somos un consumado cliente de una tienda *on-line* de



películas en formato DVD. Para hacer más cómodo el acceso a dicha web, el servidor en cuestión ha almacenado en nuestro equipo una *cookie* que le suministra cada vez que nos conectamos nuestras preferencias de compra. En esta información podría tener cabida nuestro género favorito de películas, la modalidad de pago preferida, el nombre de usuario, la contraseña y el número de la tarjeta de crédito. Si un programa malintencionado se colase en nuestro equipo, algo que no es ni mucho menos poco usual, y fuese capaz de recopilar todas las *cookies* que los distintos servidores web han almacenado en nuestro equipo, accedería a toda esta información. Por supuesto, no hace falta recordar que las consecuencias podrían ser catastróficas. Para resolver estos problemas, la *suite* integra un módulo denominado *Identity Protector*, cuya finalidad es vigilar aquellos ficheros que el usuario estime oportuno, impidiendo que terceros programas puedan acceder a ellos y, volviendo a nuestro ejemplo, sean enviados a través de Internet a máquinas no autorizadas. En realidad, el módulo *Identity Protector* es el encargado de identificar los ficheros que el usuario desea proteger, ya que quien se encarga realmente de impedir el acceso no autorizado a estos archivos es otro módulo denominado *File Guardian*.

7 Eliminar los residuos

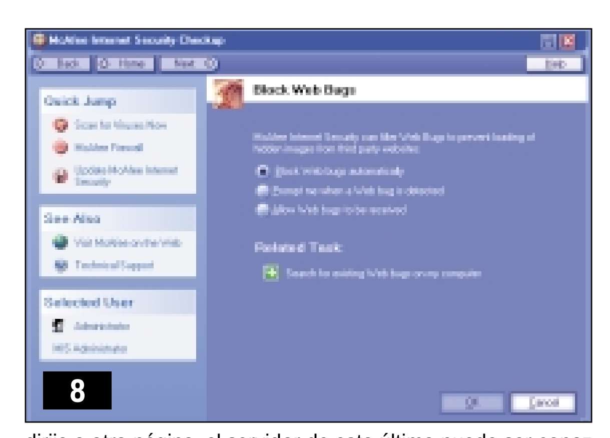
Básico

Para agilizar la navegación a través de Internet, prácticamente todos los navegadores utilizan dos recursos básicos: el histórico de páginas visitadas y la caché en disco. Gracias a la caché del navegador, la carga de páginas que han sido previamente accedidas es mucho más rápida que si tuviesen que ser de nuevo descargadas desde el sitio web original. Del mismo modo, el histórico permite a los usuarios recorrer las páginas que han visitado con antelación de forma cómoda y eficaz. Pero ambos elementos presentan un grave inconveniente: si un usuario no autorizado utiliza nuestra máquina, puede acceder con gran facilidad a toda esta información, atentando de forma grave contra nuestra privacidad. Para impedirlo y preservar estos datos de usuarios sin escrúpulos, McAfee Internet Security implementa un módulo denominado *Web Trail Cleaner* que se encarga de eliminar estos residuos de la máquina de forma automática. Las opciones que esta utilidad pone a disposición del usuario son de nuevo varias: borrado automático al cerrar el navegador o el sistema operativo (una u otra posibilidad depende del desarrollador del navegador que se encuentre instalado en la máquina en cuestión), no realizar acción alguna y, en último lugar, solicitar la confirmación del usuario antes de llevar a cabo cualquier acción. Esta última opción brinda al interesado la posibilidad de definir las páginas concretas cuyas referencias desea eliminar, tanto de la caché del navegador como del histórico.

8 Restringir información privada

Básico

Las triquiñuelas que utilizan algunos sitios web para averiguar información acerca de los usuarios que acceden a sus páginas son de lo más ingeniosas. Buena muestra de ello es el uso que ciertos servidores hacen de la URL que los usuarios teclean en su navegador. E incluso de las direcciones que no teclean. Cuando un cibernauta realiza una búsqueda de información en su motor favorito, la URL que inicialmente tecleó en la *Barra de direcciones* de su navegador, se transforma en una nueva dirección como resultado del proceso de búsqueda. Cuando a continuación el usuario haga clic en algún hipervínculo y se



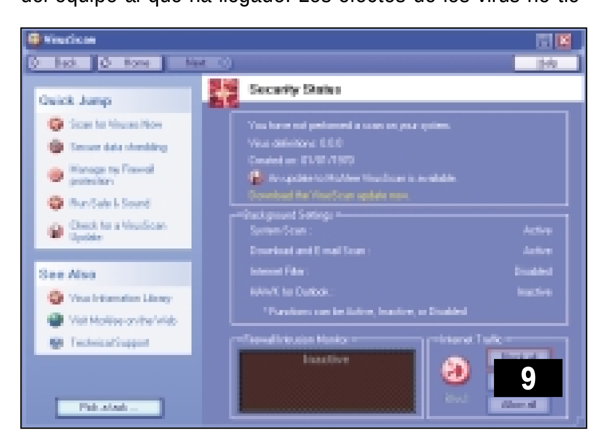
8

dirija a otra página, el servidor de esta última puede ser capaz no sólo de averiguar la página visitada previamente por el usuario, sino también cuál fue la clave de búsqueda que éste utilizó para encontrar el vínculo que le guió hasta este último sitio web. De nuevo estamos ante otro caso flagrante de atentado contra la privacidad de los usuarios. Y de nuevo McAfee ofrece otra eficaz solución integrada en la *suite* de seguridad que estamos tratando. El nombre del módulo que garantizará la privacidad de todas nuestras búsquedas es *Search Protector* y, al igual que el resto de componentes que integra la *suite*, ofrece dos opciones netamente diferenciadas: utilizar la protección durante las búsquedas (*Enable Search Protector*) y no emplearla (*Disable Search Protector*). Si el usuario opta por utilizar el mecanismo de protección, la aplicación se encargará de eliminar de forma automática la información referente a las páginas visitadas previamente antes de que pueda ser utilizada por el servidor actual, impidiendo a éste acceder a información privada. En este caso, todo será transparente para el usuario, ya que McAfee Internet Security no generará ninguna alerta.

9 McAfee VirusScan

Básico

Y por fin llegamos a uno de los módulos que sin duda resultará más familiar para la mayor parte de los usuarios: el antivirus. La popularización de Internet ha contribuido a potenciar un sinfín de excelentes posibilidades, a acercar el conocimiento y la comunicación a zonas del planeta anteriormente privadas de estos bienes, pero también ha ayudado a la expansión de los virus. Quien no sepa con certeza qué son realmente estos ingeniosos artefactos informáticos debe saber que un virus informático no es más que un pequeño programa capaz de realizar cualquier tarea a espaldas del usuario del equipo al que ha llegado. Los efectos de los virus no tienen que ser necesariamente malévolos, de hecho en numerosas ocasiones tan sólo se dedican a propagarse dejando su «huella» en las máquinas que van visitando. Pero, por desgracia, la mayor parte de los virus sí son dañinos, pudiendo llegar a eliminar ficheros del sistema y de datos, ocasionando importantes pérdidas de información y desperfectos en el software de los equipos. Las vías a través de las cuales un virus puede llegar a un equipo son múltiples. El correo electrónico es últimamente uno de los recursos más utilizados por los creadores de virus para propagar su invención, pero también es posible hacerlo de muchas otras maneras, como por ejemplo, camuflados en el interior de los ficheros comprimidos que todos los usuarios pueden descargar de forma gratuita de la Red.



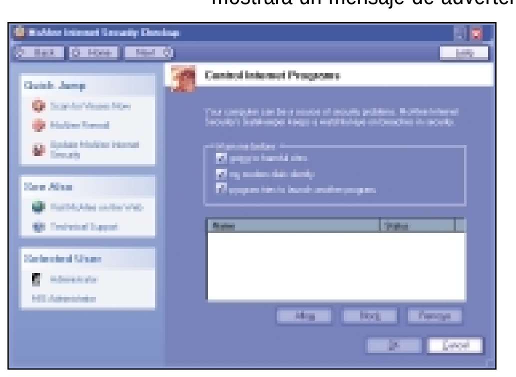
9

El antivirus que encontraremos en la *suite*, conocido como McAfee VirusScan, es uno de los más premiados a lo largo y ancho del planeta, lo que avala su elevada calidad. Para emplearlo, tan sólo será necesario dirigirse al vínculo *Scan for Viruses Now* ubicado en la zona superior izquierda de la ventana de la aplicación.

10 El *gatekeeper*

Básico

De nuevo nos topamos con un módulo de curioso nombre y utilísima aplicación. Esta vez se trata de defender nuestro equipo de la acción maliciosa de determinados controles ActiveX y *applets* Java. Para lograrlo, McAfee Internet Security mostrará un mensaje de advertencia siempre que nos conectemos a una página que incorpore cualquiera de estos elementos a priori dañinos. Muchos de estos componentes están diseñados para localizar en el disco duro del PC información privada de los usuarios y enviarla inmediatamente a través de Internet. Por este motivo, cuando el *gatekeeper* detecte una amenaza, lanzará un aviso comunicándoselo al usuario. Las amenazas que este módulo es capaz de detectar con eficacia son las siguientes: intentos de acceso a la Red no autorizados, conexiones con servidores que albergan controles ActiveX, virus y caballos de Troya, intentos de marcado utilizando el módem de forma silenciosa (para que la llamada pase desapercibida por parte del usuario) y envíos de números de identificación, entre los que pueden encontrarse los códigos de las tarjetas de crédito de las personas que utilizan la máquina.



10

11 Proteger los ficheros

Básico

Mantener a salvo los archivos que contienen información que para el usuario es vital es una necesidad que una buena herramienta de seguridad debe contemplar, y por supuesto, McAfee Internet Security lo hace. El agente encargado de velar por la seguridad de estos ficheros se conoce como *File Guardian*, una denominación que lo dice todo por sí misma. Este módulo protege a los archivos que albergan información importante para el usuario avisándole si se produce un intento por parte de alguna aplicación de acceso a través de alguna de las operaciones habituales de gestión de ficheros: apertura, renombrado, copia, cambio de ubicación y borrado. Para

que esta herramienta sea eficaz es preciso que el usuario suministre a la aplicación información acerca de qué ficheros desea monitorizar, indicándole también qué aplicaciones tienen premiso para trabajar sobre esos ficheros. Conociendo estos datos, el módulo de protección de ficheros es capaz de distinguir cuándo una aplicación desprovista de autorización accede a información protegida, impidiéndolo e informando al usuario de este hecho. Pero su eficacia no acaba aquí. En caso de que algún control ActiveX intente dar formato al disco duro, inicie un comando que pretenda realizar un borrado masivo de ficheros o lance una operación que pretenda escanear el disco duro, el usuario es avisado de inmediato a través de una alerta. En función del nivel de seguridad que el usuario seleccione durante la fase de configuración, la aplicación activará unas alertas u otras. En cualquier caso, es posible modificar la configuración inicial activando o desactivando las casillas de verificación disponibles en la ventana de la aplicación denominada *Protect files or folders*.

12 El gestor de contraseñas

Básico

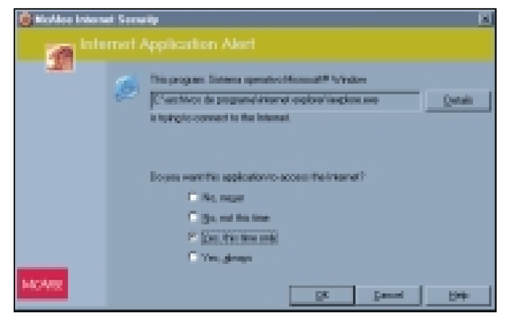
Son muchas las páginas web que precisan que el usuario que desea acceder a sus contenidos se identifique previamente. Normalmente, esto suele utilizarse en tiendas *on-line*, banca a través de Internet y operaciones similares que requieran conocer la identidad del individuo que las está realizando con el fin de procesar las anotaciones o cargos oportunos. Cuando un usuario se da de alta en varios servicios de este tipo y utiliza nombres de usuario y contraseñas diferentes, la identificación en cada uno de ellos puede tornarse una tarea un tanto engorrosa, debido principalmente a que puede resultarle difícil recordar la información apropiada en cada momento. McAfee Internet Security aparece de nuevo en escena para ayudar a todos los usuarios a gestionar sus contraseñas. Para ello, el desarrollador ha implementado en la *suite* un módulo al que ha bautizado como *Gestor de contraseñas*, gracias al cual vamos a poder almacenar de forma segura en nuestro equipo todas estas contraseñas y nombres de usuario, así como la dirección web de la página a la que están vinculadas. Para lograrlo nos dirigiremos a la ventana *Change Security Settings*, y una vez dentro de ésta a la opción *Manage my Web sites passwords*. Para introducir nuevos registros en el gestor de contraseñas haremos clic en el botón *Add*, especificando los tres parámetros mencionados anteriormente en cada uno de ellos: dirección del sitio web, nombre de usuario y contraseña. Para utilizar el contenido del *Gestor de contraseñas* tan sólo tendremos que, una vez cargada la página de identificación en el navegador, dirigirnos al *Browser Buddy* disponible en el menú contextual del icono *McAfee Guardian* (situado junto al reloj del sistema operativo), y arrastrar la información desde el gestor hasta los campos apropiados de la ventana de identificación.

12

13 Alertas de seguridad

Básico

Las amenazas que pueden originar una alerta de seguridad son básicamente dos: un intento de dar formato al disco duro y la inicialización y posterior marcación silenciosa del módem conectado al equipo. Cuando se produzca alguna de estas dos situaciones, la herramienta de seguridad mostrará una ventana en la que informará al usuario de la posible amenaza, con la finalidad de permitir que éste obre en consecuencia. La evidente gravedad de ambas se traduce en la pérdida de toda la información del disco duro en caso de que se lleve a cabo el proceso de formateo, o en la realización de llamadas a lugares indeterminados y conexiones a servidores que pueden nutrirse de información privada almacenada en el equipo del usuario. Cuando el usuario recibe una alerta que le notifica un intento de formatear su disco duro de forma involuntaria, debe apagar el equipo inmediatamente, ya que de lo contrario la aplicación que alberga el control ActiveX que está atentando contra la integridad del sistema podría completar con éxito su labor destructiva. Si la alerta informa de un intento de marcado ignorado en primera instancia por el usuario, es altamente recomendable que éste indique al gestor de alertas que debe inhibir la llamada mediante la opción *Not This Time*.

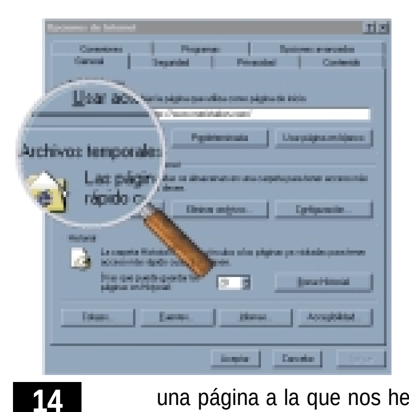


13

14 Alertas de privacidad

Básico

Tal y como hemos aclarado en apartados anteriores, una alerta de privacidad puede estar originada por cualquiera de los tres módulos siguientes: el *Gestor de cookies*, el módulo de eliminación de residuos y el administrador de contraseñas. Cuando la alerta ha sido originada por el primero de ellos, el *Gestor de cookies*, significa que un servidor al que nos hemos conectado de forma indirecta (normalmente a través de un marco descargado como parte de una página a la que nos hemos conectado de forma directa), está intentando intercambiar *cookies* con nuestro equipo. Únicamente es aconsejable aceptarlas si vamos a conectarnos a ese sitio web con frecuencia, o si son realmente necesarias para poder acceder a los contenidos en los que estamos interesados.



14

Si la alerta ha sido motivada por el módulo de eliminación de residuos, lo más probable es que previamente, durante la fase de configuración de la herramienta, hayamos especificado que deseamos ser avisados antes de proceder a la eliminación del contenido de la caché del navegador y del histórico de páginas visitadas durante la sesión de navegación (opción *Prompt to Clean Up after closing Web Browser*). La decisión en este caso debe tomarla el usuario de acuerdo con sus necesidades

y tomando como base los sitios web que ha visitado durante la sesión de navegación. Si desea mantenerlos almacenados en su máquina para visitarlos de nuevo más adelante, no deberá eliminarlos. Si por el contrario desea eliminar todo rastro de esta información del equipo para, por ejemplo, evitar que otro usuario de la misma máquina la conozca posteriormente, deberá permitir al *Web Cleaner* proceder a la eliminación de los ficheros.
Si el responsable de la alerta es el módulo de administración de contraseñas, el peligro es evidente: hay alguna aplicación que intenta acceder a los ficheros en los que almacenamos los nombres y contraseñas de usuario. En este caso la respuesta es obvia: debemos impedir dicho acceso, con la única excepción de que sea el propio usuario quien gobierna la aplicación que ha originado la alerta y sepa exactamente qué es lo que ésta va a hacer con esa información.

15 McAfee Firewall

Intermedio

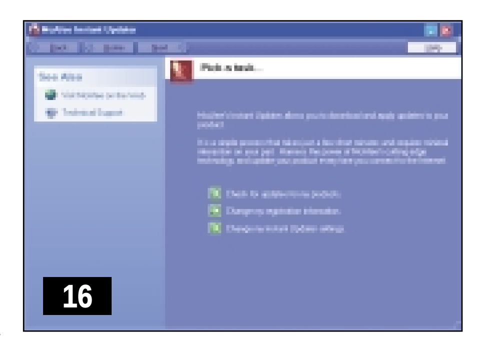
Un *firewall* es una herramienta, en este caso software, diseñada para controlar el flujo de información que entra y sale de un equipo en comunicación con un servidor web. Su propósito es sencillo: examinar todo el tráfico de información para evitar accesos no deseados al equipo. Para llevar a cabo su trabajo, el *firewall* determina si la información que está examinando cumple ciertos criterios que garantizan su inocuidad. En caso contrario, evita que ésta pueda dañar al equipo que está protegiendo.
Para iniciar el *firewall* que McAfee suministra junto a su *suite* de seguridad, deberemos dirigirnos a la ruta *Inicio/Programas/McAfee/McAfee Firewall*. La primera pantalla que aparecerá brinda al usuario la posibilidad de decidir si desea que éste filtre todo el tráfico de información, si prefiere que se bloquee tanto el tráfico entrante como el saliente o si opta por permitir la libre circulación de paquetes. La siguiente ventana permite estipular las opciones de arranque de la herramienta, siendo posible iniciar el *firewall* de forma automática durante el inicio del sistema operativo y además colocar un icono de la aplicación en la *Barra de tareas*, a través del cual será posible acceder a sus prestaciones de forma rápida. Antes de dar por finalizada la sencilla labor de configuración del *firewall*, tan sólo deberemos especificar qué aplicaciones tienen nuestra autorización para realizar accesos a Internet de forma independiente y sin previa petición de permiso por parte del usuario.

15

16 Módulo de actualizaciones

Básico

Hoy en día la mayor parte de las herramientas integran un módulo diseñado para conectarse al servidor de aplicaciones de la compañía desarrolladora con la finalidad de verificar si hay alguna actualización software disponible. Es una forma muy cómoda de mantener al día y con plenas garantías nuestro software, máxime cuando su función es proteger la integridad de la información almacenada en nuestro equipo y garantizar su privacidad. El módulo de actualizaciones de la *suite* McAfee Internet Security se ubica en la ruta *Inicio/Programas/McAfee/McAfee Shared Features/Instant Updater*. Para utilizarlo, es necesario haberse registrado previamente. Una vez que este componente haya efectuado el proceso de conexión informará al usuario acerca de la disponibilidad de nuevas actualizaciones, abordando dicho proceso de forma automática si el usuario otorga su consentimiento.


16

17 McAfee Guardian

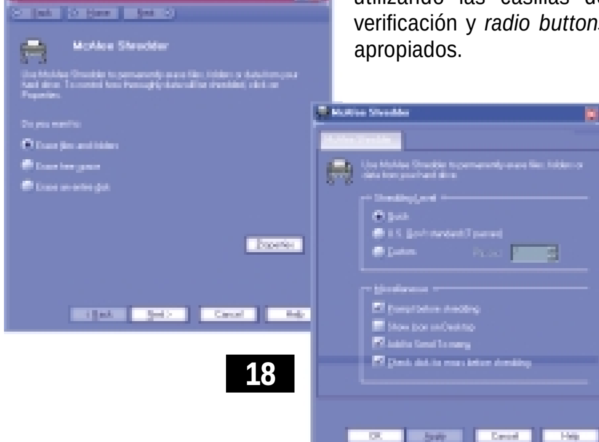
Básico

Este componente de la *suite* al que ya nos hemos referido con anterioridad no es más que un mero intermediario entre el usuario y las aplicaciones, permitiendo a éste acceder a la ventana de configuración de la herramienta de forma rápida. Se encuentra ubicado en la *Barra de tareas*, junto al reloj del sistema y, para utilizarlo, será necesario acceder a su menú contextual haciendo clic sobre él con el botón derecho del ratón. Pero no sólo va a permitirnos acceder a la ventana principal de la *suite*, sino también a un completo planificador de tareas desde el que es posible lanzar a ejecución de forma periódica cualquier aplicación instalada en la máquina. Además, desde este módulo es posible modificar la configuración por defecto del *firewall* de forma rápida y comprobar qué eventos de la *suite* están ejecutándose en segundo plano.

18 McAfee Shredder

Básico

Esta pequeña herramienta que hemos reservado para poner el broche final al artículo no es más que un sencillo y práctico gestor de espacio en disco. Con él podremos eliminar del maltrecho disco duro de nuestro ordenador toda clase de ficheros y carpetas. Incluso es posible abordar tareas de liberación de espacio en disco o realizar borrados de particiones completas.
Antes de utilizar esta herramienta para eliminar información de nuestro equipo, es preciso saber que el borrado se realiza de forma permanente. Para acceder a las opciones de configuración de la utilidad no hay más que hace clic sobre el botón *Properties*. Desde esta nueva ventana podremos determinar el tipo de borrado que deseamos utilizar y modelar el comportamiento de la herramienta utilizando las casillas de verificación y *radio buttons* apropiados.


18



Anonimato en la Red

Analizamos las claves que permiten mantener nuestra identidad oculta

La anárquica Red, por su propia filosofía, no resulta un medio excesivamente propicio, al menos en principio, para mantener nuestra intimidad. La arquitectura sobre la que se cimenta la comunicación entre máquinas permite que, bajo ciertas circunstancias y con unos conocimientos apropiados, un usuario pueda conocer la identidad y otros datos relevantes de cualquier persona que utilice los medios electrónicos para comunicarse.

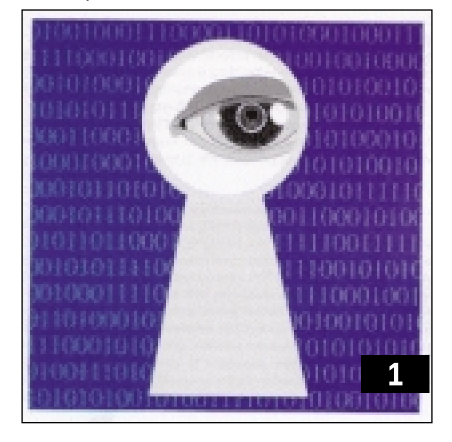


En este texto nos centraremos tan sólo en temas relacionados con el correo electrónico, una herramienta tremendamente popular y que, de nuevo, supone a menudo una vía de acceso a nuestros datos personales. Muchas veces nuestros lectores probablemente deseen mantener su identidad oculta, y para ello la propia Internet provee de varios métodos que permiten mandar y recibir correo de forma anónima. Debemos diferenciar este proceso de la utilización de mecanismos de firma digital para autentificar nuestra identidad y demostrar que los que suscriben son quienes realmente dicen ser. Analizaremos cada una de ellas de modo que podáis elegir la que creáis más adecuada para vuestras necesidades, puesto que existen métodos que permiten realizar una simple ocultación de nuestra verdadera identidad y otros que hacen muy difícil seguir el rastro de nuestros mensajes frente a posibles «curiosos» que quieran detectar de dónde proviene el mensaje origen. Por supuesto, para aumentar el grado de privacidad, se encuentran herramientas tan conocidas como PGP, el sistema que permite autentificar nuestros mensajes y que además cifra su contenido con el fin de que sólo puedan leer el verdadero contenido aquellas personas que dispongan de la clave adecuada.

1 Ocultación de la identidad

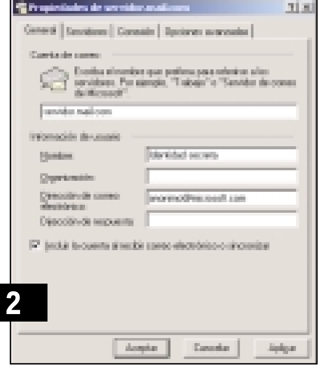
Básico

La primera de las opciones que nos permiten ocultar nuestra identidad es tan básica como limitada a la hora de asegurar el anonimato. Consiste en la modificación de nuestro nombre de remitente en los clientes de correo que utilicemos. Así, cuando configuramos las cuentas y se nos pide este dato, en vez de nuestro nombre real siempre podemos acudir a un pseudónimo o alias. Indicaremos la manera de realizarlo con dos de los clientes de correo más extendidos para Windows, Outlook Express (que viene de serie con el propio sistema operativo) y Messenger de Netscape. En ambos el procedimiento es prácticamente el mismo, y consiste en acceder a las propiedades de nuestra cuenta de usuario.



2 Cambio de identidad en Outlook

Básico



Como comentábamos, la primera de las aplicaciones en las que indicaremos cómo realizar este proceso es el conocido cliente de Microsoft. Para ello tan sólo tendremos que dirigirnos al menú *Herramientas/Cuentas* y desde el recuadro *Cuentas de Internet* que aparece, seleccionar nuestra cuenta de correo adecuada. Tras pulsar a continuación en *Propiedades,* aparecerá una nueva ventana en la que se nos permitirá modificar el nombre de usuario y la dirección de correo electrónico que aparecen. Un requisito importante a la hora de utilizar cuentas de correo ficticias a las que el destinatario pueda intentar acceder es utilizar un dominio de correo válido, como por ejemplo, *anónimo@microsoft.com*. Si

no tenemos cuidado con este detalle, Outlook se quejará al intentar enviar el correo, ya que realiza una comprobación previa de que el dominio de origen existe realmente.

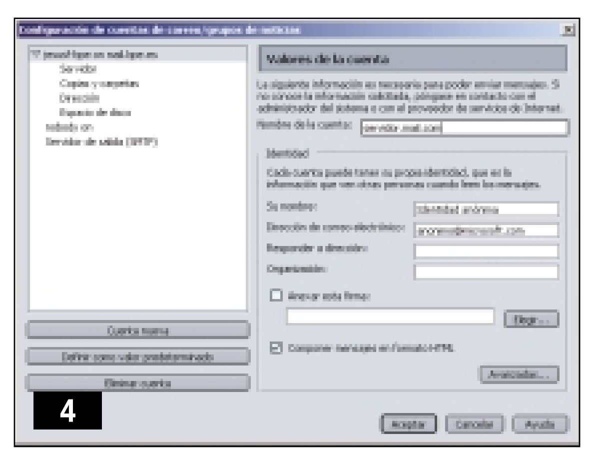
3 Comprobación del proceso

Intermedio

Una vez efectuada esta operación procederemos a la salvaguarda de los nuevos datos de nuestra cuenta y podremos efectuar una primera prueba enviándonos correo a nuestra propia dirección real. Para ello, y desde el propio Outlook, tan sólo tendremos que pinchar en *Nuevo* y escribir en la dirección de destino nuestra cuenta de correo real, por ejemplo *pcactual@bpe.es*. Al incluir texto en los campos de *Asunto* y en el propio cuerpo del mensaje, será posible ya efectuar su envío. A los pocos segundos y mediante la comprobación de la existencia de mensajes nuevos (pulsando «Ctrl + M») obtendremos como resultado la recepción de un mensaje del usuario «anónimo» desde la dirección de correo *anónimo@microsoft.com*. Por supuesto, el destinatario no podrá contestar a esta dirección de correo puesto que se trata de un *e-mail* ficticio y, en el caso de que existiera, la respuesta llegaría a un destinatario no deseado.

4 Messenger y el anonimato

Básico

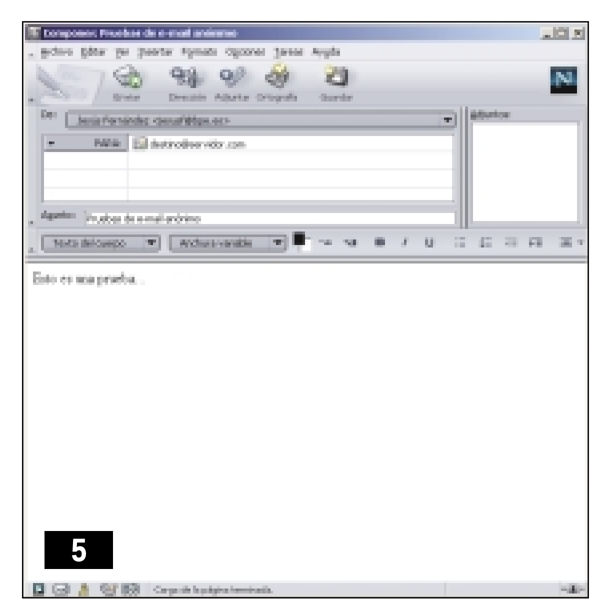


El segundo de los métodos básicos para realizar el cambio de identidad es virtualmente idéntico pero aplicado a Netscape Messenger. Por supuesto, el proceso es análogo en otros clientes de correo, aunque citamos estos dos por ser los más utilizados entre los usuarios de informática actual. Para acceder a las cuentas de correo en este programa deberemos acceder al menú *Edit/Preferences* (*Edición/Preferencias*) y procederemos a la modificación de los parámetros convenientes desde la ventana que aparece a continuación.

5 Nuevos datos

Intermedio

Al aparecer el cuadro de diálogo con la configuración de las propiedades de Messenger deberemos seleccionar en la parte izquierda la opción *Correo y noticias* (*Mail and News*) tras lo cual aparecerán en la parte derecha las propiedades correspondientes que podremos modificar introduciendo texto en los campos adecuados. Al igual que ocurría con Outlook, habrá que tener en cuenta que deberemos seleccionar una cuenta de correo ficticia (aparte del pseudónimo que quera-

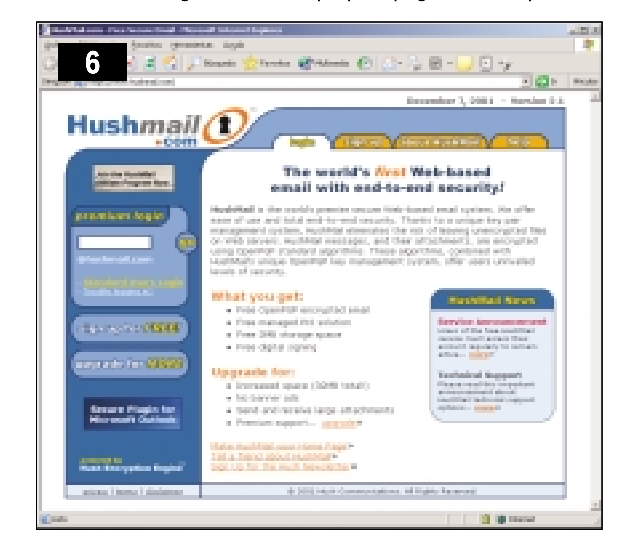


mos usar, que no debe cumplir ningún requisito especial) que, al menos, pertenezca a un dominio real, como el que poníamos de ejemplo en el truco número 2, en el que utilizamos como dirección *anónimo@microsoft.com*. La comprobación de que todo ha ido bien la podremos realizar tras la salvaguarda de los datos y el envío de un *e-mail* de prueba a nuestra dirección de correo real.

6 Utilización de cuentas de correo gratuitas

Básico

El segundo de los métodos para enviar y recibir correo anónimo consiste en la utilización de las omnipresentes cuentas de correo gratuitas que multitud de proveedores y portales de Internet ofrecen sin coste alguno. De hecho, en primer lugar contamos con las cuentas WebMail tradicionales que conceden sitios como Yahoo, Hotmail y similares; y, en segundo, se encuentran los proveedores especializados que ofrecen muchas más opciones para proteger la privacidad e intimidad que muchos usuarios demandan. La principal ventaja de estas cuentas consiste en la necesidad prácticamente ineludible de tener que acceder a ellas desde el navegador, ya que se trata de clientes integrados en las propias páginas web que, evi-

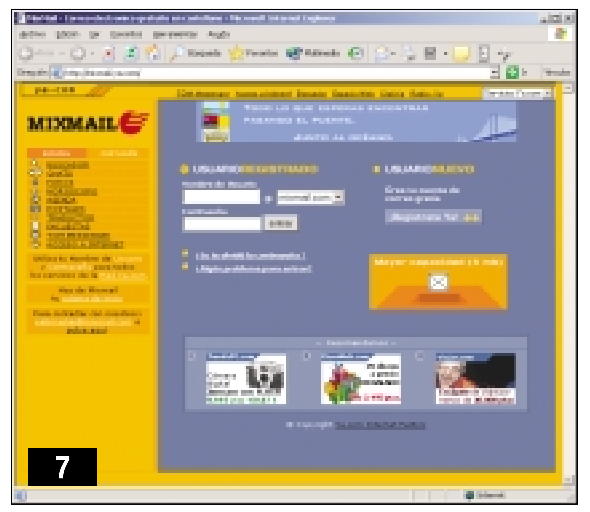


dentemente, tardan algo más en cargar los mensajes que nos han llegado. Así pues, aunque existen excepciones, normalmente no contaremos con el tradicional servicio POP3 que permite descargar los mensajes «de una sentada» para luego poder leerlos y contestarlos *off-line* hasta el momento de su envío. Las nuevas tecnologías de comunicación como ADSL y las tarifas planas telefónicas hacen mucho menos incómodo este funcionamiento, pero en cualquier caso estos clientes siempre contarán con la aparición de *banners* publicitarios que retrasan el tiempo de respuesta del sistema.

Como decíamos, frente a la utilización de cuentas de correo WebMail gratuitas tradicionales, existen ciertos servidores especializados como Mixmail, Hushmail o PrivacyX que son capaces de encriptar el contenido de modo que se establece una comunicación mucho más segura entre ambos procedimientos. El modo de registro en una de estas cuentas es muy sencillo, como indicaremos a continuación, y es muy similar entre unos servidores y otros. La gran ventaja con la que contamos en estos servicios es el grado de anonimato relativamente alto del que disponemos, ya que en ningún caso se nos obliga a introducir nuestros datos reales, aunque eso sí, los contenidos de nuestros mensajes pueden filtrarse por si el servidor considera que se está haciendo un uso ilícito de sus recursos. Algunas de las webs que permiten disponer de tales servicios son *www.hushmail.com, www.privacyx.com, www.mixmail.com, www.hotmail.com, www.yahoo.es, www.netaddress.com, www.excite.com* o *http://anonymous.to*.

7 Registro en Mixmail

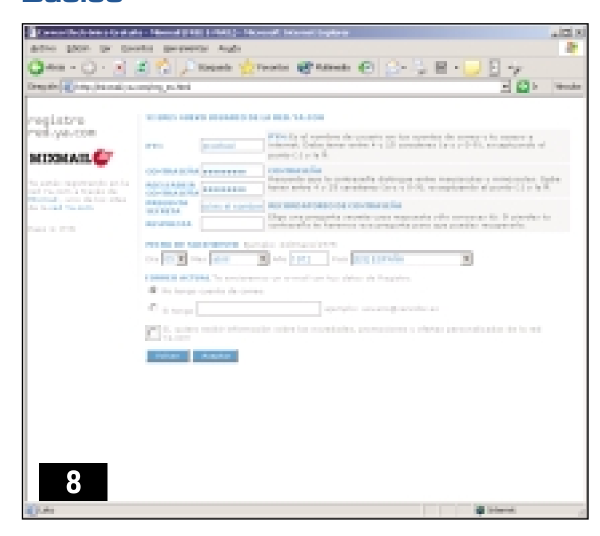
Básico



Como ejemplo para este proceso hemos tomado el servicio MixMail que, como una de sus principales ventajas, añade la interfaz en castellano, lo que sin duda agradará a los usuarios hispanohablantes. Para acceder a este servidor tan sólo deberemos contar con una conexión a Internet, y desde el navegador web teclearemos la dirección *www.mixmail.com*. En primer plano aparecerá una ventana en la que se nos pide un nombre de usuario y una *password* pero, dado que no contamos aún con ninguno de estos datos, hemos de proceder al obligado registro pulsando sobre el enlace *Regístrate ya*. En este momento aparecerá una ventana con un formulario típico en el que deberemos rellenar todos los campos correctamente. La confidencialidad de los datos está asegurada por el servicio, pero aun así muchos usuarios no desean incluir sus datos reales incluso en este formulario y de hecho mantienen a menudo un anonimato absoluto incluso para el proveedor de este tipo de servicios.

8 Activación de la cuenta

Básico

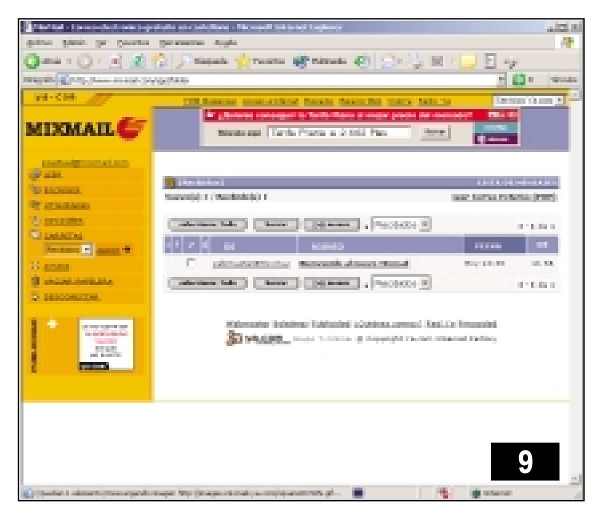


Una vez completados los campos y terminado el proceso de inscripción en el servicio, accederemos a una nueva ventana de información en la que se nos notificará que ya podremos empezar a utilizar la cuenta, bien mediante el acceso directo que figura en la página, bien mediante la introducción, de nuevo, de la página web. Pero esta vez ya contamos con nuestro nombre de usuario y nuestra *password* (que habremos elegido en el paso anterior), datos que podremos introducir en los campos correspondientes de la página de inicio de este servicio. Tras escribir ambas cadenas en sus campos y pulsar en *Aceptar*, accederemos a una nueva página web en la que se recoge información sobre nuestra cuenta de correo, con *Bandejas de entrada*, *Salida*, *Elementos enviados* y *Borrados* o bien *Borradores* de los mensajes que queramos enviar, como sucede en cualquier otro cliente tradicional.

9 Envío y recepción de mensajes

Básico

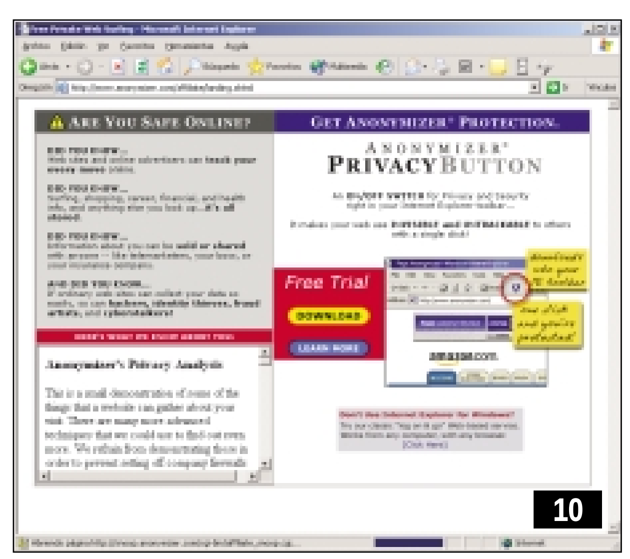
La utilización de este tipo de cuentas de correo es esencialmente idéntica a la que podremos realizar con un cliente convencional, y únicamente debemos tener en cuenta que la conexión debe ser permanente a la hora de redactar los mensajes y enviarlos. Bien, en realidad es posible tener mensajes



preparados antes de conectarnos para luego realizar la operación de *Cortar y pegar* en los cuerpos del mensaje de modo que ahorremos tiempo de conexión, un método que muchos usuarios habrán utilizado para reducir sus facturas telefónicas. El envío y recepción de mensajes se realiza pues desde los enlaces de la página principal de nuestra cuenta, que nos informa del estado de nuestro buzón de correo. Conviene tener en cuenta que estos servicios no reciben los mensajes tan rápido como pueda suceder en cuentas tradicionales POP3, por lo que es normal que un mensaje que normalmente tarde unos minutos en llegar a una de estas cuentas pueda tardar incluso horas en un servicio WebMail por la gran cantidad de información que estos manejan diariamente.

10 Páginas de envío directo

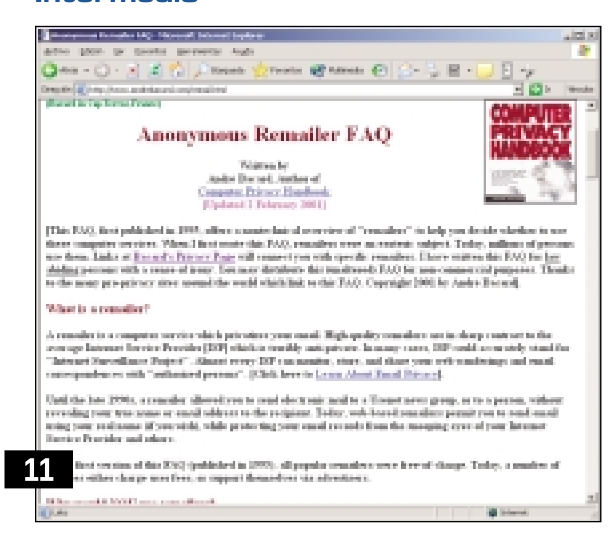
Intermedio



El siguiente método para el envío de *e-mails* anónimos es una solución mixta entre los servidores de correo WebMail y los llamados *anonymous remailers* de los que hablaremos más adelante. Esta técnica consiste en el acceso a páginas especializadas en este tipo de servicios que se encargan de la gestión de nuestros mensajes de modo que sea muy difícil trazar el camino que han seguido para llegar a destino, algo que normalmente se puede realizar con la utilización de algunas herramientas software adecuadas. Como en el caso anterior, la interfaz utilizada es la página web y, por ello, si no disponemos de una conexión continua a la Red, convendrá tener preparados los cuerpos de los mensajes (los textos en sí) para tan sólo emplear el tiempo de conexión en cortar y pegar y enviar el mensaje. Algunas de las páginas desde las que es posible acceder a tales servicios son *web.csuchico.edu/~simonian/anon.html*, *ctservice.de/taker/cgi-bin/anon-email.cgi* o la web segura del servicio Anonymizer, en *https://www.anonymizer.com/3.0/services/remailer-simple.cgi?to*. Al entrar en cualquiera de ellas, tan sólo tendremos que completar los campos de *Destinatario* (*To*), *Asunto* (*Subject*) y *Cuerpo del mensaje* (normalmente, un cuadro de texto en blanco llamado *Body* o *Text*) para a continuación enviar el mensaje a través de un *remailer* que ofrecerá al destinatario, de forma transparente para nosotros, una dirección de correo ficticia y difícil de trazar. Al utilizar estos servicios, los mensajes tardarán algo más de lo normal en llegar, ya que el proceso que se realiza al mandar un mensaje mediante este método conlleva algunas operaciones más complejas de lo habitual.

11 Remitentes anónimos

Intermedio

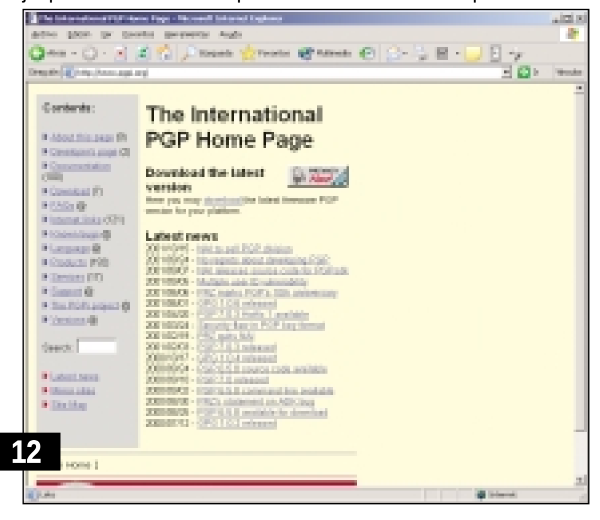


El último método que comentaremos permite mantener un alto grado de anonimato, aunque para su utilización se requieren unos conocimientos de informática mucho más profundos en todo lo referente a criptografía y seguridad. Este sistema de anonimato es utilizado por miles de personas en todo el mundo, pero su curva de aprendizaje para usuarios noveles puede resultar algo «escarpada», sobre todo si no están familiarizados con los conceptos típicos que se manejan entre los expertos en seguridad. Aun cuando la configuración de estos servicios resulta algo ardua, es el método más conveniente a la hora de mantener nuestro anonimato electrónico, ya que, averiguar los datos reales del remitente a partir de las pistas que puedan dejar estos mensajes es virtualmente una tarea de chinos.

12 *Remailers*

Intermedio

Los llamados *anonymous remailers* son centros de reenvío de mensajes en donde los correos electrónicos sufren algunos cambios que permitirán mantener nuestra identidad en secreto antes de ser enviados al destinatario. Al utilizar estos servidores, la dirección origen (la nuestra) es eliminada del mensaje para ser sustituida por una dirección correspondiente al



remailer utilizado. Existe una buena cantidad de estos centros en todo el mundo, aunque para utilizarlos debemos completar una serie de pasos no aptos para el gran público debido a la mencionada dificultad del método. Algunos programas facilitan en cierta medida estas operaciones, pero la combinación que existe entre la utilización de estos *remailers* y el programa de privacidad PGP (las conocidas *Pretty Good Privacy*) complican aún más este procedimiento.

13 Configurar la cuenta en el servidor

Intermedio



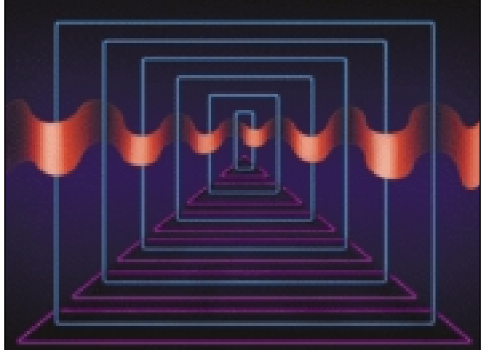
13

El primer paso es la creación de una cuenta de usuario en el servidor o *remailer*, y para ello resulta prácticamente imprescindible la utilización de PGP, ya que el método de petición de la cuenta al *remailer* consiste en la creación de nuestro juego de claves pública y privada y la utilización de la clave pública del *remailer* para a continuación componer un mensaje, bien directamente (como con un editor de texto), bien a través del software que asiste en este proceso (existen varias opciones al respecto). El mensaje, una vez completado y correctamente compuesto, se enviará al *remailer* que, si todo se ha realizado de forma adecuada, nos enviará una respuesta indicando que nuestra cuenta ya está activada y podremos proceder a utilizarla inmediatamente.

14 Utilización del *remailer*

Básico

14



Desde este momento podremos disponer de nuestra cuenta en el *remailer* para mandar mensajes de correo. La ventaja de este proceso frente a los anteriormente comentados consiste en la privacidad que se obtiene desde el primer momento, ya que únicamente el *remailer* conoce nuestra dirección de correo real. Otro punto a su favor, aún más práctico, es el hecho de que conservamos nuestra dirección de correo para recibir en ella los mensajes de los destinatarios, si estos generan respuesta. En una situación hipotética, nuestra dirección de correo real sería *pcactual@bpe.es* y, al enviar un mensaje mediante el *remailer* ésta se transformaría en *anonymous@remailer.com*. Pero lo mejor del caso es que el destinatario sí podría responder a esta cuenta, y su respuesta sería reenviada a nuestra cuenta real sin que el otro extremo conozca la dirección real de destino a la que él ha escrito, ya que todo el tráfico intermedio lo gestiona el *remailer*.

15 Tipos de servidores

Intermedio

Existen distintos tipos de servidores, desde los llamados *CypherPunk* o de tipo I, los *Mixmaster* (denominados mixtos o de tipo II), hasta los *nwenym* o *alpha*. Mientras que los *remailers* de tipo I utilizan PGP para el procesamiento de los correos, los de

15

tipo II funcionan de una manera sensiblemente distinta, utilizando el propio programa *Mixmaster* que procesa y encripta los datos mediante técnicas muy diferentes. La descripción en detalle de estos servidores se escapa del objetivo de este artículo, por lo que tan sólo queremos señalar que los programas que comentamos a continuación están preparados para varios tipos de *remailers*, de manera que cualquier usuario puede optar al que encuentra más interesante de acuerdo a la descripción de cada uno de ellos. Existen excelentes páginas de documentación al respecto que podrán ayudar a nuestros lectores, como la del experto en seguridad Andre Bacard que en *www.andrebacard.com/privacy.html* propone su visión y utilización de estos servicios. Los programas más adecuados para realizar este tipo de tareas son el conocidísimo *Private Idaho*, o aplicaciones como *Jack B. Nymble v.2*, *John Doe* o incluso la pequeña utilidad *Potato*. En todos ellos es requisito indispensable la utilización del programa PGP y, de hecho, conviene instalarse la versión 2.6.3i ya que existen ciertas incompatibilidades con las nuevas versiones de esta aplicación de privacidad con respecto a los asistentes que permiten utilizar las cuentas basadas en *anonymous remailers*.

16 *Remailers* pseudo-anónimos

Intermedio

Uno de los puntos confusos a la hora de hablar de este tipo de servicios es la diferenciación que existe entre un verdadero *remailer* anónimo y uno que, en realidad, no lo es tanto. De hecho, en la mayoría de los casos se habla de servidores totalmente anónimos que no lo son, puesto que la diferencia entre ambos tipos consiste en que, en los pseudo-anónimos se nos concede una cuenta de correo en el servidor y dependemos de la capacidad y fiabilidad de sus administradores para mantener nuestra identidad oculta. Son servicios en los que básicamente se utiliza el correo electrónico y PGP para su configuración y uso y, aunque el manejo de estos servicios es algo más sencillo, también es más bajo el grado de seguridad. Los *remailers* verdaderamente anónimos son, por ejemplo, los comentados CypherPunk y Mixmaster. De hecho, existe la posibilidad de encadenar el uso de dos o más *remailers*, de modo que la traza del camino que siguen los mensajes será prácticamente imposible de descubrir por los posibles «fisgones».

16



peligros de la navegación en Internet

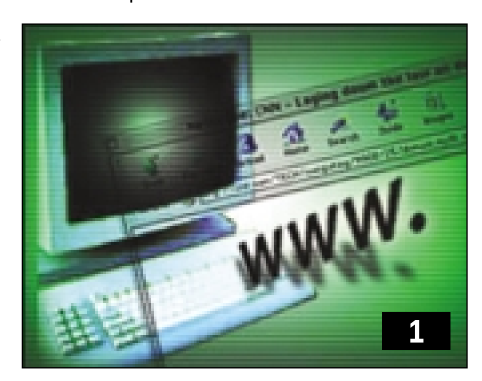
Cookies y lenguajes de *script* recogen información sin aviso

El auge de las redes de banda ancha y de la implantación final de tecnologías como ADSL o Cable ha permitido a millones de internautas acceder, por fin, y de una manera eficaz, a Internet 24 horas al día, 7 días a la semana. Las tasas de transferencia son el principal reclamo de unas tecnologías que además cada vez son más competitivas económicamente. Incluso los accesos tradicionales a través de la línea telefónica también se pueden contratar en régimen permanente, por lo que cada vez son más los usuarios que están conectados a todas horas a Internet y dejan sus máquinas encendidas.

Pero este sueño convertido en realidad entraña tantas ventajas como inconvenientes. La arquitectura de la red Internet y la filosofía cliente/servidor que prácticamente rige el funcionamiento de la gran autopista de la información conlleva ciertos riesgos. Estos peligros, por otro lado, se han derivado de intentar aprovechar mejor las nuevas tecnologías de comunicación y han partido de ideas que inicialmente estaban enfocadas al beneficio del usuario y no a su perjuicio, como en el caso de las famosas *cookies*, las «galletitas» de las que hablaremos largo y tendido, o de los lenguajes de *script* en Internet del que el protagonista fundamental es JavaScript. En ambos casos, la misma potencia que ha servido para potenciar la claridad y calidad de los contenidos ha permitido también que ciertos programadores sin escrúpulos utilicen estas herramientas, estándares de facto, para desarrollar aplicaciones que recaban información de los usuarios que éstos no desean ofrecer o incluso activan virus, troyanos y puertas traseras en nuestro PC sin que nos demos cuenta.

1 Funcionamiento de Internet

El primero de los conceptos que cualquier usuario debe comprender al internarse en Internet consiste en el propio funcionamiento de la misma. Nos centraremos en este caso en la navegación web, aunque esta parte de su utilización se extienda al resto por la pila de protocolos TCP/IP que se estableció con el nacimiento de la red de redes. Cuando navegamos por páginas web, lo que estamos haciendo constantemente es realizar peticiones de datos. Estas se realizan desde un cliente (nuestro ordenador, o más concretamente, nuestro navegador Web) hacia un servidor (el servidor Web en el que residen los datos sobre los que queremos obtener la información). Todas estas peticiones se basan en un principio en el acceso a las direcciones IP de los servidores, que a su vez saben a dónde deben responder ya que nuestros paquetes de datos ofrecen la dirección a la que se deben enviar los datos pertinentes. A partir de ese momento se establece una comunicación entre cliente y servidor y, mientras nos mantengamos en el mismo destino y naveguemos por sus páginas, la gestión de la información y su transferencia a nuestra máquina se realiza siempre desde ese mismo servidor, que simplemente traduce nuestros clics de ratón en accesos a otros enlaces de información que también es capaz de servir.



1

2 Galletas silenciosas

Precisamente debido a este tipo de comunicación anárquica, las *cookies* pueden en muchos casos llegar a ser de ayuda pero, lamentablemente, perjudicar al usuario en otros. Cuando un servidor web nos envía información que nosotros hemos demandado, también puede enviar, si así ha sido diseñado, una de estas *cookies* con información privilegiada que será útil si el mismo usuario vuelve a acceder a la página web. Lo curioso del caso es que el cliente no suele llamar la atención del usuario (nuestro navegador puede no avisarnos de que el servidor web está intentando hacer uso de estas *cookies*), y, desde luego, tampoco el sistema operativo se despeina si llega información de este tipo y se almacena, sin ningún permiso, en nuestro disco duro.



2

3 La cara vista

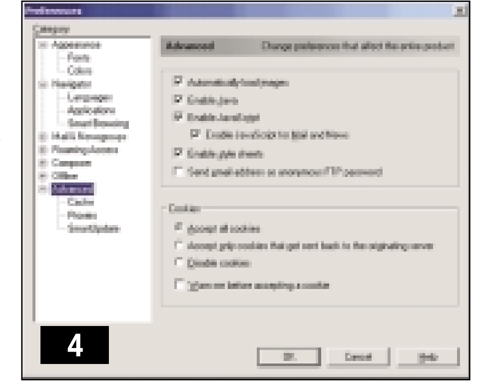
La parte visible de las *cookies*, aquella que los usuarios a menudo desconocen y que precisamente les dio sentido en un principio, es aquella que permite a los servidores de contenidos almacenar preferencias y gustos predefinidos en nuestra máquina de modo que en próximas visitas a esa dirección éste nos ahorre contenidos que «sospecha» que no nos van a interesar en base a esa *cookie*. El perfecto ejemplo lo encontramos en el comercio electrónico. Si accedemos a una página como *www.amazon.com* para comprar el DVD de La Amenaza Fantasma, éste guardará en su sistema de almacenamiento



esta acción, pero además dejará su huella en nuestra máquina con la instalación de una *cookie*. Estas «galletas» no son a menudo más que simples ficheros de texto con cadenas que permiten identificar al servidor ciertas preferencias en próximas visitas. En nuestro caso, si desconectáramos y volviésemos a conectarnos a Amazon días más tarde, el servidor comprobaría si existe alguna *cookie* en nuestra máquina que él mismo hubiera dejado, la compararía con su base de datos y a continuación nos ofrecería, por ejemplo, una página principal en la que se mostrarían DVD y CD de audio con las bandas sonoras de las películas de Star Wars. Este ejemplo se extiende virtualmente a todos los portales de contenidos de Internet, que precisamente centran su éxito en complejos mecanismos de minería de datos (*Data Mining*) e Inteligencia Artificial para fidelizar a los clientes y usuarios de sus servicios.

4 Dos etapas de funcionamiento

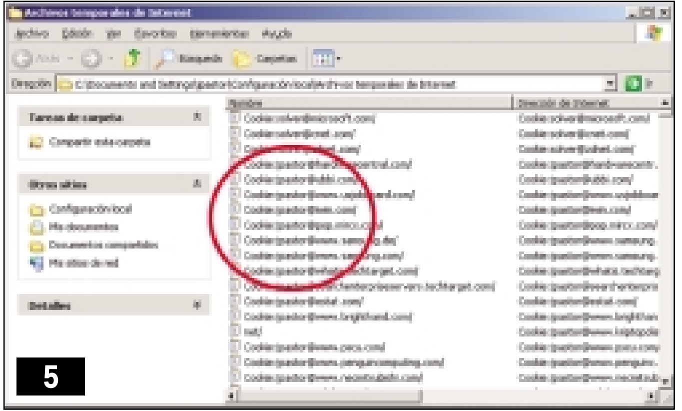
Como venimos comentando, la instalación y uso de *cookies* se puede dividir en dos etapas. En la primera de ellas, la «galleta» se almacena en nuestra máquina sin nuestro consentimiento previo, guardándose en este fichero preferencias que se han deducido de nuestra navegación por la página web del servidor, pero también información relevante, por ejemplo, sobre nuestra máquina y el software que utilizamos para la conexión y navegación por Internet. Si nuestro navegador tiene activada la aceptación de estos ficheros (lo que ocurre por defecto en todos ellos), este archivo se guardará en una lista de distintas *cookies* a las que el navegador tiene acceso, y de la que extraerá información el servidor web más adelante, tras haberla guardado en nuestro disco duro sin permiso.



En la segunda etapa, la *cookie* se transmite de forma automática y sin nuestro conocimiento al servidor web una vez nos conectemos a él. Lo más sorprendente del caso es que, por extraño que parezca, almacenaremos *cookies* en nuestro disco duro de páginas que ni siquiera hemos visitado.

5 ¿Cómo ha llegado esto aquí?

Desde Windows XP, si uno accede al *Explorador* de archivos y se dirige a la carpeta donde se almacenan las *cookies*, se encontrará con muchas sorpresas. En nuestro ejemplo, esta carpeta se encuentra en *C:\Documents and settings\Nombre de Usuario\Cookies*. Al abrirla, nos encontraremos con un primer fichero *index* que se asemeja al «cookies.txt» utilizado en versiones anteriores de Windows, seguido de un buen montón de pequeños ficheros de menos de 1 Kbyte. Todos ellos se caracterizan por llevar una arroba para identificar al usuario al que se le han generado, seguido por un identificador del servidor origen. A primer golpe de vista observamos que muchos de ellos ni nos suenan, pero desde luego otros ni siquiera deberían estar. Por ejemplo, sin duda muchos de nuestros lectores contarán con una de las *cookies* más extendidas, proveniente del servidor de *banners* publicitarios DoubleClick. Nunca hemos entrado en DoubleClick, y sin embargo, ahí está esa «galleta» que almacena información que nosotros desconocemos. Si lo abrimos, no resolveremos ninguna duda, pues-



to que simplemente consta de una larga cadena alfanumérica sin sentido. Por lo tanto, ¿qué ha pasado? Simplemente, que la propia filosofía anárquica de Internet nos ha jugado una mala pasada. Aunque no se trate de algo grave, alguno de los *sites* a los que hemos accedido contiene *banners* cedidos por DoubleClick, que a cambio conoce que nosotros hemos accedido a esta página y genera publicidad orientada a nuestros gustos de forma transparente y sin que nos enteremos de nada. Un usuario que visite páginas literarias se encontrará, cuando navegue por otras, que se le muestran páginas de tiendas de libros o accesos a webs con los últimos *e-books*. Un curioso informático que «trastee» y busque información especializada en páginas técnicas se verá navegando por páginas en las que los conocidos reclamos hagan referencia a otras tantas páginas de hardware y software especializado que estén asociadas con Double Click. ¿Es esto bueno o malo? La decisión y el poder de cortar este tipo de usos los tiene, en la mayoría de los casos, el propio usuario.

6 Limitaciones de las cookies

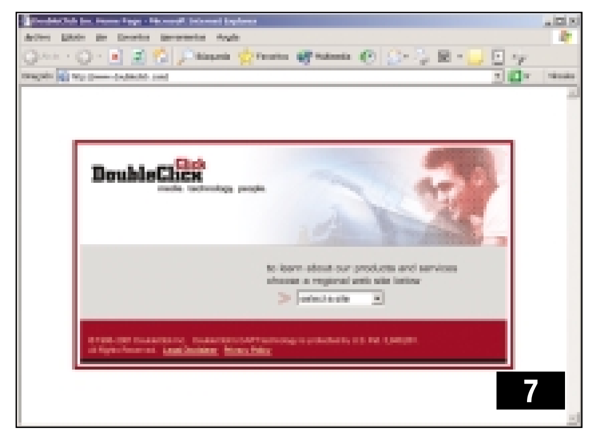
A pesar de la tremenda polémica que suscitan, lo cierto es que estos pequeños ficheros no son en realidad tan dañinos, y casi se podrían considerar como una pequeña molestia frente a los verdaderos peligros que pueden ocasionar Java, JavaScript,



6

ActiveX o los pequeños CGI, lenguajes dinámicos de los que hablaremos más adelante y que pueden ser aprovechados (y de hecho, lo son) para atacar vulnerabilidades en diversos sistemas operativos. Centrándonos en estas «galletas», hay que tener en cuenta que existen una serie de limitaciones que las *cookies* no pueden superar. Son ficheros que deben tener como máximo 4 Kbytes y, un número no superior a 300 en el directorio en el que se almacenan, cumpliéndose el principio FIFO (*First In, First Out*, es decir, sale el más antiguo) si llega una nueva *cookie* cuando ya había 300. Además, existen un máximo de 20 *cookies* por servidor o dominio, de modo que no podremos tener 21 o 300 «galletitas» provenientes de DoubleClick. Además, y esto es importante, los servidores no pueden acceder a *cookies* que ellos mismos hayan almacenado. Es decir, DoubleClick no podría «ver» la información relevante que haya podido almacenar en otra *cookie* Amazon, por poner un ejemplo.

7 Posibles amenazas



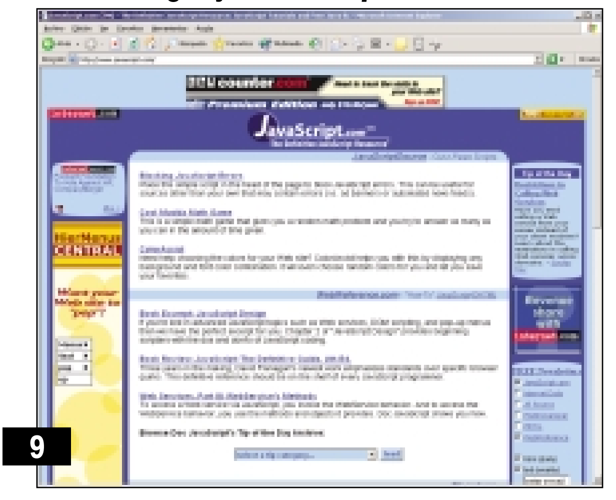
7

El problema con estos ficheros es que la información que almacenan puede ser visible para los navegadores web (ya Internet Explorer ocasionó serios problemas porque cualquier servidor acabó pudiendo acceder a estas informaciones), y aunque los servidores web puedan consultar teóricamente sólo sus *cookies* a través de estos navegadores, cualquier usuario que pertenezca a nuestra red (si es que estamos conectados a una) podrá acceder a ellas y, a partir de las mismas, determinar cierta información relevante como nombres de usuario y contraseñas a, por ejemplo, webs de comercio electrónico.

8 El cazador cazado

Por todas estas razones, hay que terminar indicando a este respecto que las famosas *cookies* han pasado de ser un mecanismo que teóricamente fue implementado para favorecer al usuario en uno que lo que ha hecho ha sido beneficiar a los anunciantes. Aunque suene repetitivo, el caso de DoubleClick es famoso porque existe un proyecto en el que están incluidas importantes organizaciones que protegen la privacidad en contra del funcionamiento actual de este sistema. La IETF (*Internet Engineering Task Force*) y la organización EPIC (*Electronic Privacy Information Center*) se han aliado contra este método que, según ellos, atenta contra la privacidad de los usuarios, y de hecho la IETF ha propuesto en un RFC (*Request For Comments*), la número 2.109, una solución al problema. Para ampliar esta información os recomendamos que acudáis a páginas con ingentes recursos en todo lo referente a *cookies* y privacidad como son Cookie Central (*www.cookiecentral.com*) o la propia EPIC (*www.epic.org*) o la IETF (*www.ietf.org*).

9 Lenguajes de *script*

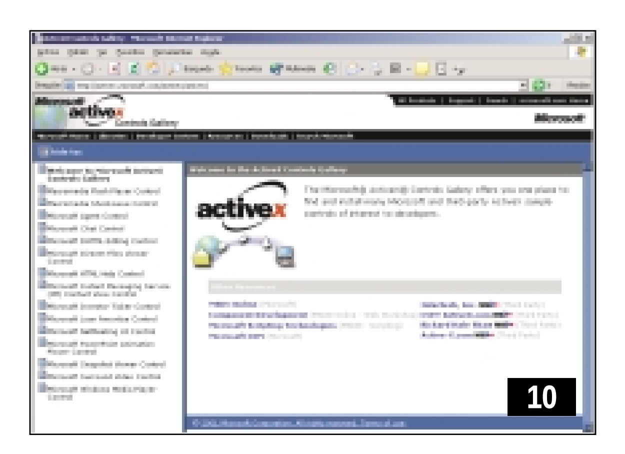


9

Gran parte de la potencia de Internet se basa en la utilización de los nuevos lenguajes de programación que hacen de las páginas web un medio dinámico que se va «creando» a sí mismo. Gracias a las características de Java, JavaScript, ActiveX y a las de los propios *plug-ins* y CGIs que pueden añadirse a una página, es posible realizar verdaderas maravillas que hagan que un sitio web casi se autogestione a sí mismo y sirva información de manera autónoma, además de automatizar procesos y extraer información de las propias visitas. Pero de igual modo, las posibilidades de estos lenguajes hacen que hayan surgido multitud de agujeros de seguridad en los navegadores actuales que se aprovechan de la filosofía de estas aplicaciones para, por ejemplo, acceder a nuestros discos duros y extraer información de los mismos sin que nos demos cuenta.

10 ActiveX

Entre los componentes más que reconocidos de estas vulnerabilidades se encuentran los controles ActiveX, que ofrecen tal control sobre la máquina que los está ejecutando que Microsoft tuvo que ponerse manos a la obra para proteger este tipo de transacciones de alguna manera. ActiveX permite acceder a información sensible incluso integrándose con las aplicaciones que generan ese tipo de datos, para aprovechar las debilidades de la aplicación y transferir (a donde el creador del control Active X lo desee) datos de cualquier tipo, que van desde nombres de usuario y contraseñas a números de tarjetas de crédito y fechas de caducidad de las mismas. Para evitar el problema se creó *Authenticode*, un mecanismo de firma digital que permite verificar al destinatario de la transac-



ción. Junto a estas firmas digitales han surgido las llamadas autoridades de certificación, que actúan como notarios en este tipo de proceso y que asignan certificados digitales a particulares y empresas para que éstas puedan dar fe de sus operaciones sin riesgo para el cliente.

11 Java

Probablemente esta es una de las palabras a partir de las cuales uno asocia a Internet. Java se ha convertido en el estándar de facto en millones de páginas web en todo el mundo, que utilizan este lenguaje de programación orientada a objetos como pilar básico de su estructura interna. La sintaxis, muy similar a la utilizada en C++, hacía que los anteriores programadores no tuvieran mayor dificultad en migrar hacia este lenguaje, que además contaba con una característica muy especial. Sun lo desarrolló para que fuera totalmente independiente de la plataforma, y por esta razón se le conoció como uno de los primeros lenguajes interpretados, aunque en realidad tome parte de esta filosofía y parte de la tradicional en la que los



códigos fuente de las aplicaciones deben producir previamente código objeto que pueda ser ejecutado. A diferencia de ActiveX, Java fue concebido para, al menos en principio, proteger ciertos recursos del sistema, manteniendo el campo de acción del código a las llamadas *sandboxes*, mediante las cuales la responsabilidad de la seguridad ejecutada pasa a ser confiada al software y no al usuario, que teóricamente no debe preocuparse por nada. Esto en realidad no es así ya que, como en tantos otros casos, Java ha dado muchos quebraderos de cabeza a los desarrolladores de navegadores de Internet, que han visto cómo el propio concepto de Java permitía aprovecharse de ciertas características del lenguaje (y, evidentemente, del navegador web) para realizar operaciones ilegales en nuestro sistema. Aun así, Java sigue evolucionando día tras día y se trata de uno de los lenguajes que mejor están orientados a ofrecer tanta potencia como seguridad para el usuario final y, de hecho, es una de las alternativas más fiables a la hora de diseñar *applets* que aumenten la capacidad de respuesta de nuestro sistema.

12 JavaScript

Tan potente como polémico, JavaScript se ha convertido en uno de los recursos con más posibilidades de la gran autopista de la información. La gran cantidad de opciones que posibilita este lenguaje lo hacen apto para muchos usos beneficiosos, pero por las mismas razones se convierte en el número uno de la navegación segura en Internet debido a tres posibles peligros primordiales. En primer lugar, los *scripts* generados en JavaScript pueden «robarnos» la cartera y transferir a cualquier otro lugar datos relevantes de nuestros discos duros, incluidas contraseñas o claves de encriptación que utilicemos para cifrar nuestros contenidos. La invasión de nuestra intimidad y privacidad es el segundo de los inconvenientes, ya que Javascript puede ser usado para espiar nuestro bagaje durante el tiempo que estemos conectados y mantener una relación exacta de los sitios que hemos visitado o de los ficheros que hemos descargado. En tercer lugar, es uno de los lenguajes (junto a VisualBasic, otro de los protagonistas en esta faceta) que más relación tienen con la aparición de gusanos, virus y troyanos que se derivan de la utilización del correo electrónico como medio de comunicación.

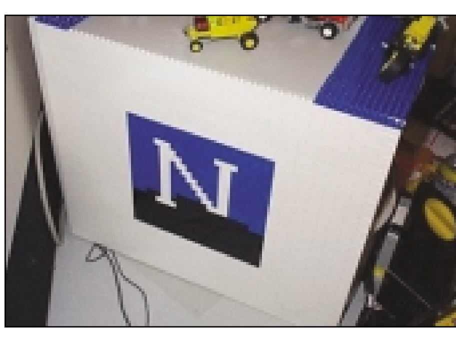
13 Alternativas a JavaScript

Los expertos a seguridad indican que las tareas que se realizan con JavaScript (tradicionalmente, la gestión del diseño de la página y la manipulación de formularios) pueden ser controladas con otros lenguajes más seguros. Entre ellos señalan a **Perl** como la alternativa perfecta para la manipulación de datos y su validación en páginas web. En segundo lugar, **PHP** permite a los diseñadores de páginas web hacer todo cuanto JavaScript permite, pero de una forma más segura y además mejorando la conectividad con bases de datos en nuestro sistema. Por último, Java es el complemento perfecto para la creación y gestión de contenidos dinámicos en páginas web además de dotar al internauta de cierta protección frente a código «malicioso».

13

14 Las opciones en los navegadores

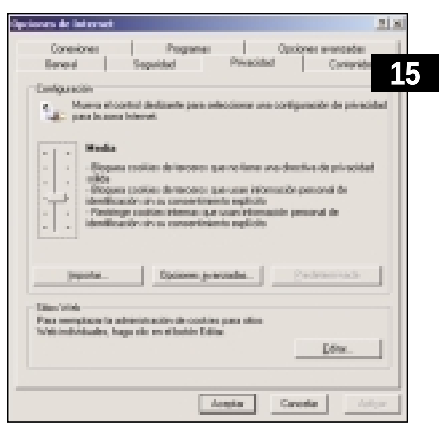
La mayor parte de los peligros que acechan a los internautas tradicionales se centran en el uso de los propios navegadores. Por mucho que estas aplicaciones traten de velar por la seguridad de nuestros datos, ciertas páginas web pueden estar diseñadas de manera que se acceda a información privada o incluso algo peor. Por esta razón analizaremos a continuación las medidas de seguridad que se han tomado en las últimas versiones de los dos navegadores estrella en la actualidad, Internet Explorer 6.0 y Netscape 6.2. En ambos casos se ha mostrado especial interés en el apartado de la seguridad y privacidad en Internet, siendo incluso Explorer más potente en cuanto a las distintas opciones de configuración en este sentido. En ambos casos, la protección se basa en la activación de los permisos de ejecución para los distintos lenguajes que pueden suponer algún riesgo para el usuario y, curiosamente, en los dos podremos encontrar extensa información sobre el funcionamiento de las *cookies* y de su control con los gestores que incluyen ambas aplicaciones.



14

15 Control de *cookies* en Explorer

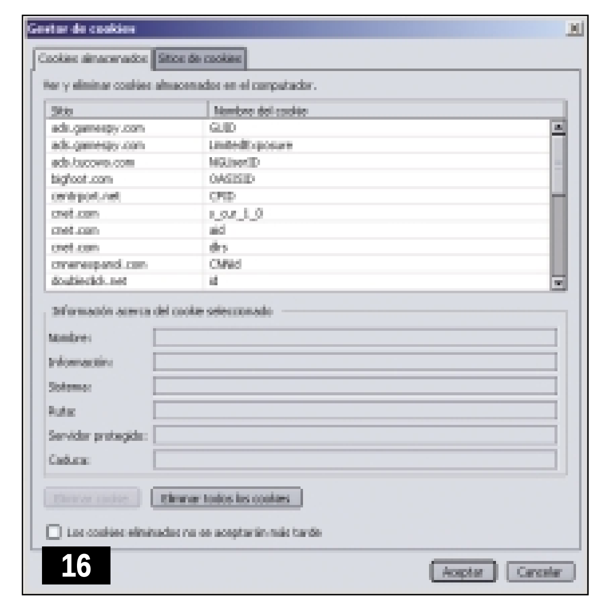
La gestión de las famosas galletas de Internet es bien sencilla desde Explorer, aunque la interfaz es algo más engorrosa que en el caso de Netscape. Para acceder a este tipo de tarea nos vamos al menú *Herramientas/Opciones de Internet*. Desde la nueva ventana que nos aparecerá pulsamos en *General* y a continuación tendremos dos opciones. Si queremos borrar todas las *cookies* presentes en el sistema tan sólo deberemos pulsar con el botón izquierdo del ratón en el botón *Eliminar cookies*. En caso contrario, podremos analizar el contenido de las mismas en *Configuración*. Una vez en la siguiente ventana pulsaremos sobre *Ver Archivos*, con lo que nos aparecerá la ventana en la que es posible observar los ficheros temporales que Explorer ha almacenado en nuestro disco duro, y que van desde las típicas imágenes GIF y JPEG hasta pequeñas rutinas JavaScript y ficheros «.class» de Java. Y, por supuesto, las *cookies*, que aparecerán con el apelativo *«Cookie:»* seguido de nuestro nombre de usuario en todas ellas. Si no deseamos almacenar alguna, la seleccionamos y eliminamos como cualquier otro archivo. Este control personalizado tiene también su complemento en las directivas de seguridad que permiten aceptar unas *cookies* y desechar otras, o hacer que la aplicación nos pregunte antes de aceptar cualquiera de ellas. Para establecer estas directivas deberemos acceder de nuevo al menú *Herramientas/Opciones de Internet* y desde la ventana siguiente acceder a la pestaña *Privacidad* en la que nos aparecerá una barra de desplazamiento con la que fijaremos las propiedades específicas en este apartado.



15

16 Control de *cookies* en Netscape

El *Gestor de Cookies* de Netscape es aún más intuitivo y fácil de utilizar que el presente en Internet Explorer. En este caso, para llegar a esta utilidad tendremos que acceder al menú *Editar/Preferencias*. En la parte izquierda activaremos el menú desplegable que aparece tras pulsar la opción *Privacidad y seguridad* , y a continuación, señalaremos la opción *Cookies* para acceder a sus propiedades. Aquí podremos observar en

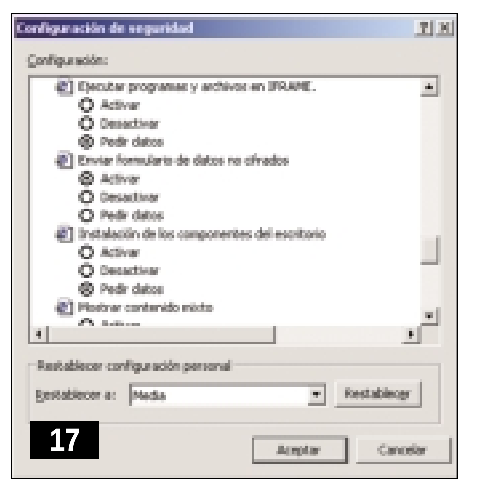


16

la parte superior de la ventana las opciones de configuración en lo que se refiere a la aceptación de estos pequeños archivos (más completa en Explorer, eso sí), y, en la parte inferior, el botón *Ver Cookies guardados* que dará paso al comentado *Gestor de Cookies*. La información que nos muestra esta nueva ventana permite conocer la información relevante de cada una de las *cookies* que Netscape haya almacenado en nuestro disco duro a petición del servidor web que hayamos visitado, y podremos eliminar ésta o incluso todas ellas «de golpe y porrazo» pulsando sobre la opción *Eliminar todos las cookies*.

17 Formularios y componentes

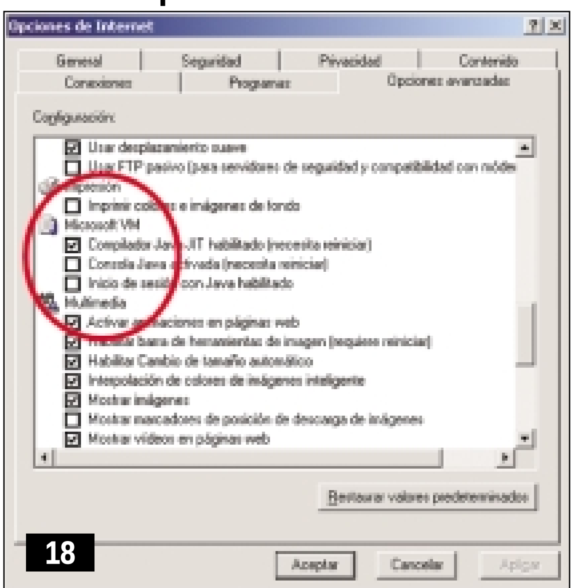
Entre las opciones disponibles en las utilidades de configuración de ambas aplicaciones se encuentran aquellas que permiten vetar el uso de formularios (basados normalmente en CGIs, que también entrañan cierto riesgo para el usuario) o la instalación de componentes para el navegador. También se indica en Explorer el control sobre los controles ActiveX con bastante profundidad, algo que sin embargo en Netscape no aparece (lógico, puesto que este tipo de mecanismos han sido desarrollados por MS, rival de Netscape). Las opciones de validación y manejo de certificados digitales también está ampliamente cubierto en ambas herramientas, y no nos extenderemos en su utilización ya que este apartado se escapa del objetivo de este artículo. Sin



17

embargo, hay que hacer notar que para poder acceder a dichas propiedades deberemos, en MS Internet Explorer, pulsar sobre *Herramientas/Opciones de Internet*. A continuación, seleccionamos la pestaña *Seguridad* y seleccionamos el icono marcado como *Internet*. Si tras seleccionarlo pulsamos en la parte inferior de esta ventana en el botón *Nivel personalizado,* nos aparecerá una ventana con todas las opciones de configuración en este sentido. De manera análoga, en Netscape debemos acceder a las preferencias de la aplicación mediante el menú *Editar/Preferencias* para a continuación seleccionar la opción *Privacidad y seguridad*, pero esta vez y a diferencia del paso anterior en el que mostrábamos el apartado para *cookies*, podremos realizar cambios en la configuración que rige el comportamiento del gestor de formularios, de contraseñas o a las opciones referentes al uso de certificados, seguridad basada en las capas SSL o validación de nuestra identidad a partir de los mecanismos de los que Netscape hace uso.

18 Desactivar Java y JavaScript en Explorer

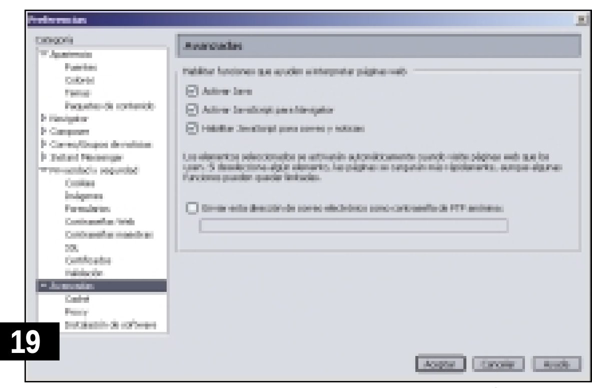


18

Si queremos acceder a una navegación prácticamente exenta de peligros, tendremos que pensar seriamente en la eliminación de componentes Java y JavaScript de las páginas web que visitemos. Esto hará que ni siquiera podamos acceder a ciertas páginas totalmente desarrolladas mediante estos lenguajes, pero también evitará que podamos llevarnos sorpresas desagradables durante nuestros paseos por la Red. Para desactivar estas opciones que por defecto no lo están en ningún navegador, deberemos de nuevo acceder al menú de configuración de Internet Explorer mediante el acceso a *Herramientas/Opciones de Internet*. Una vez aparezca la nueva ventana, pulsamos sobre la pestaña *Opciones avanzadas*, lo que nos llevará a otra ventana en la cual podremos desactivar la opción adecuada en la parte baja del menú de opciones, en la sección marcada con el nombre *Microsoft VM* (de *Microsoft Virtual Machine*). Si desactivamos todas las opciones Java y reiniciamos el navegador habremos vetado el acceso a páginas con este tipo de contenidos.

19 Netscape, Java y JavaScript

Mediante un procedimiento similar pero algo más sencillo podremos realizar el mismo tipo de operación en Netscape 6.1. En el menú *Editar/Preferencias* nos desplazamos por la



19

parte izquierda de la ventana y señalamos la opción *Avanzadas*. Ojo, la señalamos, que no significa que despleguemos sus opciones pulsando sobre la flecha que está situada a la izquierda de este texto *Avanzadas*. Al quedar resaltada esta opción, aparecerán en la parte derecha las tres opciones que permiten o no la utilización de código Java y JavaScript. Así pues, tan sólo tendremos que desactivar estas casillas para asegurarnos de que, al menos en este apartado, no corremos peligro al navegar por Internet.

20 Conclusiones

Después de la lectura de este artículo, quizás algunos usuarios se plantearán seriamente el uso de un navegador de Internet como lo hacían anteriormente. Es evidente que la propia arquitectura de Internet y los pilares sobre los que se asienta el desarrollo de los servidores de contenidos, cualesquiera que estos sean, puede poner en peligro nuestros propios datos personales. El grado de privacidad que uno quiera conseguir dependerá de lo confidencial que considere los datos, pero por mucho que lo intentemos, y como señalan muchos expertos en seguridad, es prácticamente imposible estar conectados y ser completamente anónimos, o no estar expuestos a los riesgos que la red de redes provoca. Cuanto más seguros queramos estar de nuestra propia intimidad, más limitaremos nuestra experiencia como internautas y, dadas las circunstancias actuales, la aparición de *bugs* y agujeros de seguridad en servidores web parecen hacer peligrar cada vez más la seguridad y confidencialidad de los datos de los usuarios. Sin embargo, estos errores se producen por el estado de desarrollo continuo al que están sometidos estándares, aplicaciones y tecnologías usadas en el proceso por lo que, si queremos disfrutar de contenidos y servicios que puede llegar a ofrecer Internet y los que en ella trabajan, mucho nos tememos que habrá que atenerse a las consecuencias.


20



El intermediario de la Web

Descubre cómo evitar intrusos mientras navegas

Cada vez que nos conectamos a un servidor web nuestro navegador envía información sobre nuestra identidad y nuestro sistema sin que nos percatemos. Aunque es posible evitar este tipo de «chivatazos», estaremos siempre ligados al mecanismo que utilizamos para conectarnos a la Red, el protocolo TCP/IP. Dado que es necesario establecer una forma de enviar y recibir datos entre nuestro equipo y los que proporcionan la información, es necesario revelar uno de los datos más interesantes y peligrosos: nuestra dirección IP. A partir de ésta es perfectamente posible conocer nuestra situación geográfica, además del ISP que utilizamos. Si la dirección IP asignada por este último es fija, caso por ejemplo de las líneas ADSL que es posible contratar con Telefónica, la situación se torna aún más grave. Esta información queda registrada en los servidores web y puede utilizarse para reunir un auténtico compendio sobre nuestras actividades en Internet.



Puede existir además un ingrediente que hace significativamente más peligroso navegar por la Web. Si nos encontramos en un sitio público, por ejemplo un cibercafé, o nuestra oficina, la salida a Internet puede estar controlada e incluso filtrada. En los cibercafés puede ocurrir que el dueño del negocio espíe a sus clientes, en busca de números tan interesantes como la tarjeta de crédito o datos personales. En las oficinas la situación es bien diferente: imposibilitar que consultemos determinadas páginas web durante horas de trabajo no es demasiado complejo con el software adecuado. Espiar a los empleados para comprobar su «dedicación» durante este periodo tampoco.

Pese a estos peligros, existen formas de evitar, o al menos intentarlo, que ni los servidores web se percaten de nuestro paso por ellos, o que el equipo que nos proporciona la salida a Internet (también llamado *gateway*) sean espías inexcusables.

Los dos métodos que vamos a comentar hacen uso de una técnica comúnmente empleada para espiar: utilizar un intermediario. Si en lugar de recurrir directamente a un servidor central empleamos la ayuda de un servidor intermedio, el *gateway* de nuestra red simplemente verá que se establece una comunicación entre nuestro equipo y un servidor aparentemente inocuo. Dado que existen tecnologías capaces de inspeccionar los contenidos, es decir, examinar el contenido de las páginas web u otros ficheros recibidos (con independencia de donde procedan), en muchas ocasiones se establece una conexión cifrada entre nuestro navegador y el intermediario de forma que éste no pueda entrometerse.

Existen dos tecnologías, los intermediarios web y el *proxy* «de toda la vida». Los primeros suelen ofrecer muchos añadidos, como por ejemplo, cifrado o tratamiento de *cookies*, mientras que los segundos son más simples de utilizar. A continuación os mostramos una relación de varios lugares, servidores y páginas para evitar ojos curiosos.

Saltar de web en web

La forma más vistosa de evitar que alguien se entrometa en nuestros hábitos de navegación es utilizar otras páginas web intermedias. Los servicios ofrecidos por estas suelen ser de carácter gratuito, aunque la gran mayoría de ellos disponen de diversos servicios con mayores ventajas bajo la modalidad de suscripción. Sin duda alguna, lo mejor es la posibilidad de cifrar todo el tráfico entre nuestro equipo y el servidor web que hace de intermediario. Esto evitará que programas destinados a capturar y analizar todos los paquetes de la red deduzcan lo que realmente nos traemos entre manos, de hecho ni siquiera el administrador del cortafuegos que se encuentra en nuestra oficina se enterará de nada. Habitualmente también son capaces de eliminar ciertos contenidos «peligrosos», como por ejemplo código JavaScript, *cookies*, e incluso algunos *banners* publicitarios.

www.anonymizer.com

Sin duda una de las páginas más conocidas de este mundillo. Además del filtrado web cuenta con algunos servicios interesantes, de pago, y por supuesto, de uno gratuito. Tan sólo tenemos que introducir la dirección de la página y pulsar el botón *Go* adyacente para asegurarnos que las páginas son filtradas de contenido potencialmente peligroso, esconder nuestra dirección IP, y evitar el seguimiento entre *sites*. Lo realmente interesante de sus servicios es un pequeño añadido (*Privacy Button*) que se instala junto con Internet Explorer y permite activar y desactivar la redirección pulsando un botón en la barra de menús del navegador. También podremos configurar las opciones de filtrado con mayor detenimiento desde esta misma localización.



El único problema viene dado por la limitación de ciertas páginas en la modalidad gratuita, algo que no debería presentar problemas si nos dirigimos a servidores poco conocidos.

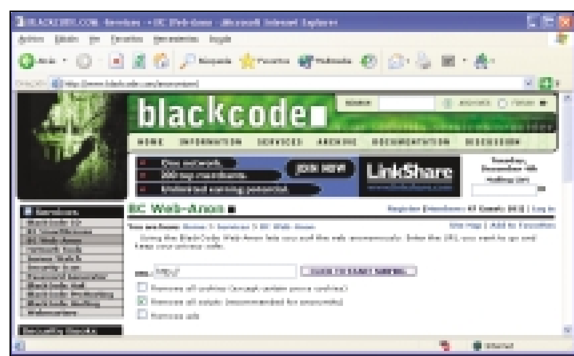
www.megaproxy.com

Si no estamos dispuestos a pagar un duro por asegurar nuestra privacidad, Megaproxy ofrece servicios de forma gratuita que en otras páginas necesitan algún tipo de suscripción. Este es el caso del cifrado SSL entre nuestro equipo y sus servidores. Dispone además de posibilidad de «engañar» al sistema de *cookies* de forma que las páginas que las requieren para su correcto funcionamiento no presentarán problemas a la vez que mantendrán nuestro anonimato. Otras ventajas de la página son la aceleración de la descarga de ficheros HTML (utilizando un pequeño sistema de «limpieza») y la vigilancia de los contenidos de una forma bastante atenta. Esta última inspección nos avisará cuando el motor de filtrado no pueda asegurarse de «limpiar» completamente las páginas de elementos peligrosos. Para evitar que la dirección inicial se transmita sin ser codificada previamente, un útil enlace permite ver la página



de inicio mediante el protocolo SSL. Durante nuestra navegación aparece en la parte superior de la ventana una pequeña barra donde, además del logo de la compañía, se encuentran controles que reemplazan a los de Internet Explorer. Junto a estos, un *banner* permite el uso de este servicio excelente sin «rascarse el bolsillo».

www.blackcode.com



Tras esta página cuyos contenidos están dedicados a la seguridad y hackers, se encuentran diversos servicios. Desde la URL *www.blackcode.com/anonymizer* un sencillo botón nos permite navegar de forma anónima. El motor es capaz de eliminar las *cookies* por completo, con la excepción de aquellas que permiten funcionar con *proxy*, además de los *scripts* e imágenes publicitarias. En algunas ocasiones será recomendable desconectar por completo JavaScript, utilizando para ello las opciones de nuestro navegador para aumentar la seguridad.

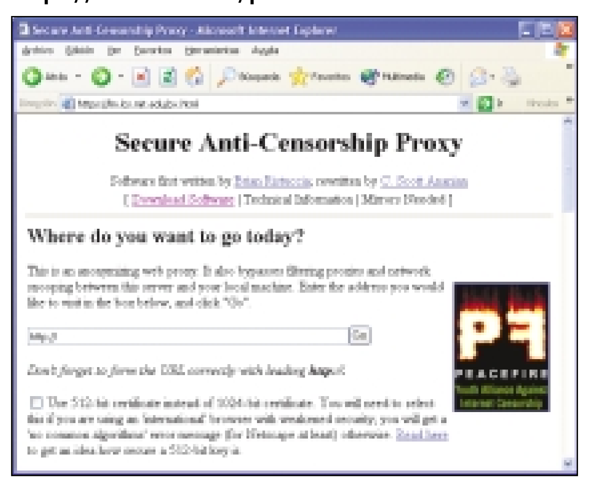
www.idzap.com



Al igual que ocurre con Anonymizer, esta compañía ofrece la posibilidad de recurrir a servicios de pago o conformarse con los gratuitos, algo más limitados. Al contrario que la mayoría, es necesario crear una cuenta de usuario incluso si accedemos a la modalidad libre de pago. El servicio básico sólo actuará como filtro entre nosotros y el servidor, bloqueando las *cookies* y *javascript*. Por otro lado, IDsecure, de pago, es capaz de cifrar las comunicaciones, ocultar datos a nuestro

antojo (por ejemplo, el bloqueo de la dirección de la última página visitada), acceder a sitios protegidos mediante contraseña e incluso cifrar nuestro historial de visitas. Para más comodidad, la publicidad en forma de ventanas *pop up* puede eliminarse.

https://lm.lcs.mit.edu/px.html



Fruto de una tesis, esta página es mucho más interesante por sus contenidos que por su capacidad de evitar el filtrado indiscriminado de página de algunas organizaciones. Su simpleza lo dice todo: solamente tenemos que teclear la dirección que queremos visitar y pulsar el botón *Go*. Previamente tendremos que aceptar la advertencia que Internet Explorer nos muestra al encontrar un certificado digital del que no tiene conocimiento. Mucho más interesante es el enlace que nos permite descargar el código de la aplicación. De esta forma, todos aquellos que quieran instalar un sistema como este en su propio ordenador lo tendrán fácil, sólo es necesario compilar bajo Linux.
Como peculiaridad, también puede ser utilizado como *proxy* convencional para lo que debemos introducir la dirección del servidor.

www.ponoi.com

Su nombre quiere decir «privado» en Hawai, sin embargo en Internet viene a decir mucho más. Tras su cuidado diseño se esconde una de las páginas más útiles que hemos visto. Utiliza un mecanismo que se asemeja a un *proxy* convencional, y el servidor está instalado en nuestra propia máquina, por lo que es necesario descargarlo antes. No obstante, el proceso se realiza de forma automática y casi completamente transparente al usuario por lo que es bastante difícil despistarse. Una ventana en la parte inferior proporciona acceso a los tres servicios básicos de los que dispone: acceso a web seguro, almacenamiento de ficheros remoto y gestión de contraseñas. Todos ellos utilizan cifrado fuerte para evitar malas intenciones de terceros. Los dos últimos, toda una novedad en la lista, permiten almacenar hasta 10 Mbytes y gestionar todas las contraseñas que vamos creando en nuestras visitas diarias en las diferentes páginas que requieren un registro. Esta es sin duda una de nuestras favoritas.

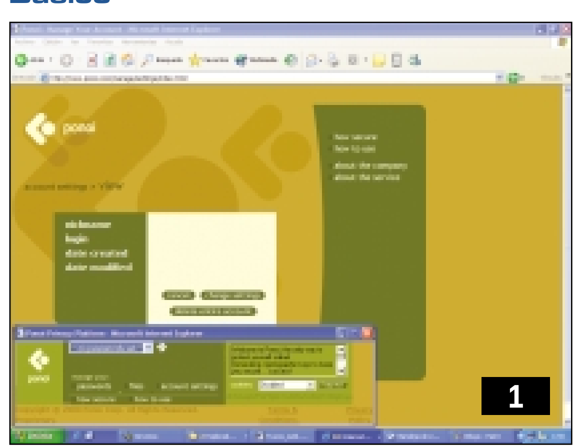


Proxy convencional

La otra tecnología que podemos utilizar es ya vieja conocida por muchos de nosotros. En muchas oficinas se utiliza precisamente para lo contrario: forzando a todos los clientes a utilizar esta salida se filtran determinados protocolos, como por ejemplo HTTP o FTP, facilitando esta tarea. Al tratarse de un intermediario más siempre podemos acudir a él para evitar que en los registros de los servidores web aparezca nuestra dirección IP. Debemos tener en cuenta una consideración antes de lanzarnos a cambiar los parámetros de nuestro navegador: no todos los servidores necesariamente tienen por qué ocultar los datos de nuestro equipo. Es conveniente tener mucho cuidado. Además puede darse el caso de que la dirección escogida muestre publicidad en forma de *banners* o que éste filtre determinados contenidos por cuestiones morales o legales.

1 Comprobar un *proxy* anónimo

Básico



Antes de lanzarnos a navegar con seguridad es recomendable asegurarse de que, al menos, nuestra dirección IP se oculta al resto del universo. Podemos recurrir a *www.multiproxy.org* en donde hallaremos un enlace que nos permite visualizar los datos que el servidor web es capaz de recoger por el simple hecho de conectar. Si nuestra dirección no se encuentra entre estos, estamos de enhorabuena. En esta página encontraremos además una larga lista de servidores, a los que podemos unir los de *www.proxylist.com* o *http://tools.rosintrument.com/proxy*. Encontraremos otras muchas fuentes, frecuentemente cambiantes, en Internet. Algunas direcciones serán realmente públicas, sin embargo en otras ocasiones podemos encontrarnos con que estamos accediendo a través de servidores privados, por lo que es necesario cierta prudencia.

2 *Multiproxy*, saltando entre anónimos

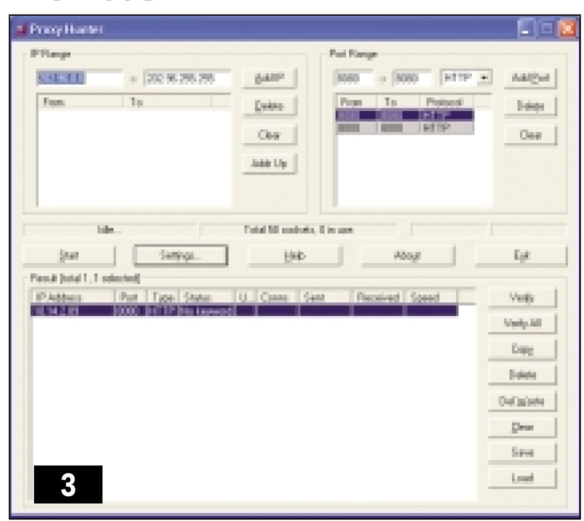
Intermedio

La mejor forma de evitar que nos sigan la pista es utilizar varios *proxies* intermediarios para descargar una única web. Al realizar las peticiones desde diferentes servidores de forma simultánea estamos provocando que el seguimiento sea realmente com-

plejo. Dado que esto es imposible sin recurrir a una aplicación externa utilizaremos Multiproxy. Con este programa (que podemos descargar de forma gratuita desde *www.multiproxy.com*) esquivaremos la mayoría de los registros de los servidores sin más problemas. Tras descomprimir e instalar la aplicación hemos de configurar como servidor *proxy* en el navegador la dirección 127.0.0.1 y el puerto 8088. Tras esto renovaremos la lista de servidores que contiene el programa desde la web utilizando una de sus opciones y seleccionaremos *Check all*, dentro del menú *Proxy List*. Con esto se verificarán de forma automática si los servidores que utilizamos son realmente anónimos y disponen de conexión. Hecho esto, debemos considerar que aquellas páginas que detecten nuestros datos utilizando *JavaScript* o Java no son filtradas, por lo que es mejor desconectar estas opciones dentro de nuestro navegador.

3 Buscar nuestro propio *proxy*

Avanzado



Si buscamos nuevas formas de salir a Internet sin tener que recurrir a las ya muy cribadas listas de equipos, siempre podemos realizar nuestras propias búsquedas. Este paso que aquí comentamos puede ser interpretado por algunos administradores como intrusión, cuando en realidad no es más que una prueba de puertos dentro de un rango de direcciones. Si aún nos atrevemos a continuar con la búsqueda necesitaremos una herramienta adecuada que encontraremos en *www.world-net-news.com/phutn.exe*. Para su empleo solamente requiere especificar un rango de direcciones IP y posibles puertos a probar. La pequeña aplicación se encargará de verificar si en cada una de las direcciones proporcionadas se encuentra un *proxy*. Se trata también de una excelente herramienta perfecta para verificar otras posibles «salidas» a Internet desde una intranet a veces ocultas.

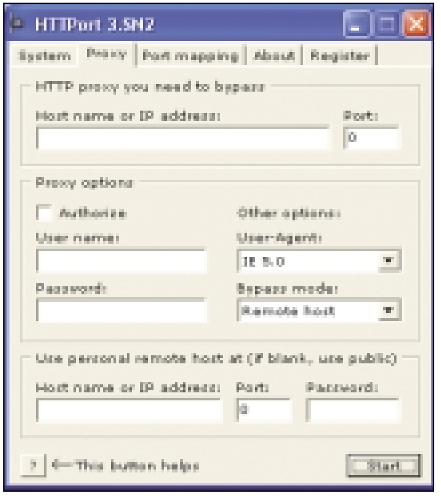
4 Redirección completa

Avanzado

Si estamos dispuestos a esquivar por todos los medios el *proxy* que espía nuestras comunicaciones, todavía tenemos una oportunidad. Gracias a HTTPort podremos utilizar todas nuestras aplicaciones que utilicen puertos diferentes al HTTP, aun cuando la política de seguridad corporativa lo impida. Entre sus características más interesantes se encuentra la que nos permite cifrar el tráfico entre nuestro equipo y el servidor que redirecciona nuestro tráfico (llamado HTTHost). Comenzaremos instalando el programa (que podéis encontrar en *www.htthost.com*). Basta con introducir la dirección del *proxy* que vamos a esquivar (y el puerto a través del que enviar la información). Si es necesario introducir una contraseña para acceder a éste, también podremos utilizarla (e incluso hacer pasar el programa por Internet Explorer, Opera o Netscape a voluntad). A continuación debemos elegir el modo de redirección de los dos disponibles. Disponemos de un método cifrado y uno sin cifrar, por lo que elegiremos el cifrado. Para terminar basta con introducir la dirección IP del equipo en el que hemos instalado el servidor HTTHost.

5 El servidor

Avanzado



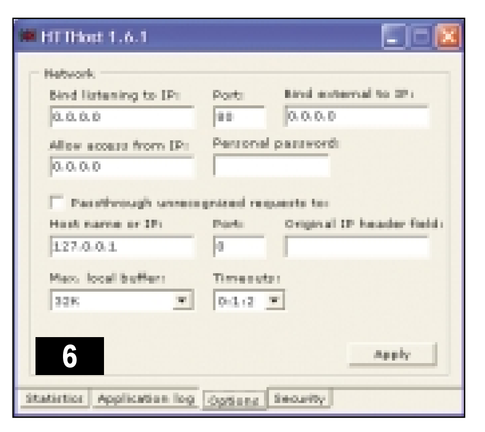
HTTHost requiere descomprimir el fichero y ejecutarlo para comenzar a funcionar. Sus opciones de configuración son bastante simples. Hemos de especificar la dirección IP «de escucha», a la que se conectará HTTPort, y la que reenvía el tráfico. Si no queremos que otros utilicen nuestro ordenador como equipo redirector, también podremos especificar la dirección IP de nuestro *proxy*, de forma que será posible el acceso desde este además de una clave.

Aunque el tráfico entre este servidor y HTTPort esté cifrado, hemos de tener en cuenta que las claves utilizadas para ello son las mismas para todo el mundo por lo que es posible descifrarlo sin más problema. Si queremos unas claves diferentes, tendremos que comprarlas desde la página web de la aplicación (*www.httport.com*)

6 Aplicación práctica de HTTPort-HTTHost

Intermedio

Aunque parezca de funcionamiento complejo, su puesta en marcha es lo suficientemente simple como para que desde nuestra oficina, donde Internet está filtadro y vigilado, podamos navegar y utilizar todo tipo de programas sin cortapisas. Si en nuestra casa disponemos de un ADSL, sólo hemos de configurar el módem para que redirija todo el tráfico del puerto 80 al ordenador en el que hemos instalado HTTHost, el cual debe permanecer encendido. En la oficina tomaremos nota de las opciones del navegador y las introduciremos en HTTPort, además de la dirección IP del equipo de nuestra casa que habremos averiguado previamente. Con esto, por fin seremos libres.





Comunicación confidencial

Cómo cifrar nuestros mensajes

Ya os hemos mostrado cómo navegar por Internet de forma anónima. No obstante, en ocasiones nos interesará más mantener la confidencialidad de nuestras comunicaciones. Cada vez que enviamos un paquete a un servidor a través de Internet, éste puede llegar a recorrer un largo trecho hasta su destino. A lo largo de ese camino alguien que se mantenga a la escucha acabará, antes o después, interceptando datos críticos. Si somos los administradores de un equipo y no tenemos otra opción que gestionarlo a través de una red insegura, las cosas se pueden complicar aún más. El mero hecho de transmitir una clave y nombre de usuario de una cuenta privilegiada puede suponer la pérdida del control del equipo. Y dado que la mayoría de los protocolos que normalmente utilizan las aplicaciones no cuentan con seguridad alguna, transmitir un fichero utilizando nuestra sencilla y familiar herramienta FTP es una locura si el contenido de éste es confidencial. La solución pasa, cómo no, por cifrar todo aquello que no queramos que caiga en manos ajenas. Las posibilidades son múltiples, pero si nuestro presupuesto es algo limitado, el número de las mismas decrece. A continuación os mostramos diferentes técnicas utilizadas para comunicar dos equipos y conseguir que cualquier byte que se intercambie entre ellos sea un mero dato aleatorio para aquellos que escuchan a lo largo del camino.

1 Un servidor SSH

Básico

Directo desde los entornos Unix, OpenSSH no es más que la implementación Open Source de uno de los protocolos seguros más conocidos: SSH (de Secure Shell). Sin duda alguna, entre los mejores que encontramos rastreando la web se encontraba OpenSHH on Windows, que podemos descargar desde *www.networksimplicity.com/openssh*. De esta página descargamos, de momento, dos aplicaciones: el servidor y el *addon pack*. La instalación resulta trivial, tan sólo hay que poner en marcha el fichero ejecutable. Este copiará a nuestro ordenador los componentes cliente y servidor, generando tras esto y de forma automática las claves públicas y privadas necesarias para realizar la comunicación.

2 Cómo añadir usuarios

Intermedio

El siguiente paso resulta menos obvio que el anterior. Para que los usuarios puedan acceder al sistema, será necesario comunicarle de alguna forma quiénes y de qué forma pueden acceder a éste. Al tratarse de una traducción casi directa de un sistema Unix, aquellos familiarizados con sus conceptos se encontrarán con la existencia de varios directorios y ficheros muy familiares. Se trata de los directorios *\var* y *\etc* y el fichero *passwd*. Para conseguir que un usuario acceda al sistema utilizando este método, tendremos que dirigirnos al directorio donde instalamos la aplicación y llamar a la herramienta *Mkpasswd*. Tenemos que tener en cuenta que la autenticación final la efectúa Windows, por lo que, para que un usuario acceda a una línea de comandos Windows, éste debe estar dado de alta en la máquina con anterioridad. De igual forma, es posible utilizar los usuarios del dominio para el acceso a la máquina. Ahora que ya sabemos qué usuarios dar de alta, examinaremos el fichero *passwd* que se encuentra dentro del directorio */etc*. Allí encontraremos tras la instalación dos usuarios creados: *Administrator* y *nt_user_name*. No debemos eliminar ninguno de los dos, sin embargo el primero tiene una utilidad muy concreta: impedir que el administrador pueda acceder a través de este método. Para añadir nuevos usuarios, nos dirigiremos al directorio *\ssh* y teclearemos: *mkpasswd –l –u usuario >..\etc\passwd*. La primera opción define el tipo de usuario que estamos añadiendo, en este caso local. Si fuéramos a añadir usuarios del dominio tendríamos que haber utilizado *-d*. A continuación con *-u* especificamos el usuario que vamos a añadir. Finalmente, enviamos la salida del programa al fichero de contraseñas. Si accedemos a este fichero veremos cómo aparecen varias líneas que especifican el usuario y otros parámetros.

Hay que resaltar que para que el sistema tenga en cuenta los nuevos usuarios tendremos que detener el servicio y volver a arrancarlo. Si continuamos sin poder darnos de alta, será necesario reiniciar el equipo.

2

3 Detener el servicio sin reiniciar

Avanzado

Si consideramos que no es aceptable detener la máquina cada vez que añadimos o eliminamos un usuario del servicio, todavía existe otra alternativa. Podemos recurrir a una de las herramientas más conocidas para Windows NT y 2000. Desde *www.systeminternals.com* descargaremos un pequeño paquete de aplicaciones (no llega al Mbyte) llamado Pstools. Dentro del mismo encontraremos programas que, muy al estilo Unix, permiten eliminar procesos desde la línea de comando. Los que más nos interesan son Pslist (muestra los procesos en ejecución) y Pskill (los elimina). Su uso es bastante sencillo dado que sólo es necesario introducir el nombre de los procesos a eliminar: *sshd* y *Firedaemon*. Tras la eliminación sólo tendremos que volver a iniciar el servicio desde el controlador situado en *Herramientas de Administración*. Este mecanismo tiene una razón de ser: aun cuando detengamos el servicio, casi siempre queda residente el programa *sshd*, por lo que detenerlo (ya sea desde el gestor de servicios o utilizando *net stop "openssh server"*) no es suficiente. Además, si utilizamos el *Administrador de tareas* para eliminar el proceso *sshd* puede pasar que, de las múltiples copias en ejecución, alguna quede residente, lo que casi siempre lleva a la confusión y fallos a la hora de cambiar la configuración.

4 Conexión desde un cliente

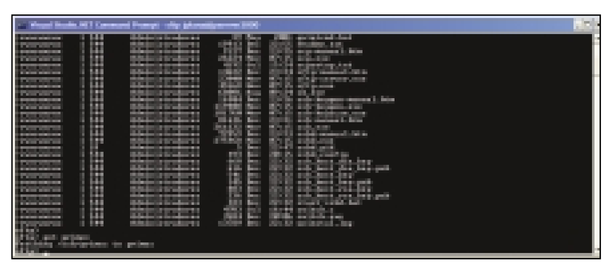
Intermedio

El mismo fichero que descargamos para instalar el servidor contiene los ficheros que son utilizados para el cliente. Una vez copiados los archivos al sistema, abriremos una línea de comandos y desde el directorio en el que efectuamos la instalación llamaremos a la aplicación. Como parámetros introduciremos el nombre de usuario seguido de una arroba y el nombre del equipo (o dirección IP) donde queremos acceder. Si seguimos todos los pasos correctamente, principalmente en el lado del servidor, nuestro cliente nos advertirá que desconoce la clave pública del *Host* y nos preguntará si queremos añadirla a nuestro repositorio. Afortunadamente nos enseñará también la «huella» (*Fingerprint*) de la clave, para asegurarnos todavía más. Si aceptamos la clave, el programa nos volverá a pedir otro dato, esta vez la clave de acceso. Introducida correctamente, nos encontraremos con una línea de comandos segura conectada directamente al servidor.

5 Transmitir ficheros

Intermedio

Otra de las aplicaciones que han hecho de OpenSSH un éxito consiste en la transmisión de ficheros de forma segura, para lo que se emplea SFTP. La conexión es, básicamente, idéntica a la de SSH. La diferencia estriba en el resultado: en lugar de aparecer una interfaz de comandos, nos encontraremos con una herramienta muy similar al FTP tradicional. La transmisión de los ficheros en ambos sentidos es en esta ocasión cifrada, lo que permite enviar y recibir archivos sin temor alguno.



5

6 Determinar el directorio de entrada en SFTP

Avanzado

Cuando ejecutemos SFTP por primera vez, nos daremos cuenta de que entraremos directamente al directorio en el que se instala la aplicación. Existe una forma de evitar esto, de forma que podamos redirigir a los usuarios directamente. Para ello tendremos que editar el fichero *passwd* que se encuentra en el servidor, en el directorio *\etc*. Al abrirlo, veremos una serie de líneas que, como ya explicamos, determinan los permisos de cada uno de los usuarios. Distinguiremos cada usuario porque su línea comienza por su nombre de entrada. Los diferentes campos están separados por el símbolo «:» y el campo que buscamos se encuentra entre el quito y sexto símbolo. Como

6

veréis en el ejemplo, entre ellos aparece */ssh*, directorio que tendremos que sustituir por el que nosotros queramos. Existen un par de reglas para completar este campo. En primer lugar, tenemos que cambiar todas las barras del directorio utilizadas en Windows (\) por las empleadas en sistemas Unix (/). Y en segundo lugar, todas las rutas son relativas al directorio principal de la unidad en la que hemos instalado el programa, por lo que si queremos utilizar otra unidad diferente (por ejemplo hemos instalado el programa en C: y queremos que los usuarios accedan a F:), tendremos que utilizar una notación especial. Así, si queremos especificar un directorio en la unidad H: tendremos que comenzar la ruta con */cygdrive/h/*.

7 Copiar ficheros

Básico

Entre las herramientas más sencillas de este paquete se encuentra SCP (*Secure Copy Protocol*). Con él podremos copiar ficheros entre un servidor y nuestro equipo utilizando la línea de comandos y usando el canal cifrado proporcionado por SSH. Si queremos copiar un fichero de nuestro equipo al servidor, sólo tendremos que utilizar algo parecido a la siguiente línea: *scp fichero usuario@servidor:/ruta/*. Si necesitamos especificar una unidad diferente en el servidor, por ejemplo copiar el fichero «texto.doc» al directorio *F:\prueba\textos*, utilizaremos una sintaxis como esta: *scp texto.doc usuario@servidor:/cygdrive/f/prueba/textos/*.

Para copiar un fichero desde el servidor a nuestro equipo, tan sólo tendremos que invertir el orden de los parámetros: *scp usuario@servidor:/ruta/fichero /ruta/local/*.

El parámetro adicional *-C* colocado antes que el resto de opciones permite comprimir el texto, algo especialmente útil si enviamos un fichero de gran tamaño no comprimido previamente.

8 Cómo eliminar la contraseña

Avanzado

Muchos administradores cuentan con *scripts* y otros métodos para automatizar muchas de las tareas cotidianas. Uno de los requerimientos suele consistir en la transmisión de ficheros entre dos equipos, trabajo con frecuencia efectuado utilizando

el simple y llano cliente TFTP (*Trivial File Transfer Protocol*). Con la herramienta SCP es posible efectuar casi la totalidad de estos trabajos, con la ventaja adicional que supone disponer de unas comunicaciones cifradas.

Por otro lado, en ocasiones nos gustaría ahorrarnos teclear la contraseña cada vez que establezcamos esa conexión, ya sea SCP, SFTP o la simple línea de comandos. OpenSSH dispone de un mecanismo que, sin truncar la seguridad inherente en el sistema, permite obviar la contraseñas de acceso. Se trata de la **Autenticación mediante clave pública/privada**.

Para que el mecanismo funcione correctamente, tendremos que seguir una serie de pasos, sobre todo en el lado del servidor, antes de poder utilizarla. En primer lugar será necesario que detengamos el servicio OpenSSH y eliminemos los procesos (con Pskill). A continuación tendremos que modificar el fichero *passwd* y cambiar el UID (número que se encuentra tras el segundo símbolo «:») por 500. También será conveniente crear un directorio propio para el usuario.

De esta forma, los usuarios que vayan a utilizar este tipo de autenticación dispondrán en el fichero de contraseñas de una entrada similar a esta:

Jose::500:513::/cygdrive/c/users/jose:/ssh/switch, donde el directorio personal de *Jose* se encontrará en *C:\users\jose*. Dentro de éste además crearemos una carpeta llamada *.ssh*.

Para terminar con la configuración editaremos el fichero *sshd_config* y nos aseguraremos de que contiene una línea como esta: *StrictModes no*.

Antes de reiniciar el servicio, nos dirigiremos al equipo desde el cual vamos a acceder al servidor. Desde éste llamaremos a la aplicación *SSH-keygen* utilizando el parámetro *-d*. Dejando todas las preguntas que nos hará el sistema en su valor por defecto, habremos creado dos ficheros que contienen nuestra clave pública (*id_dsa.pub*) y la privada correspondiente (*id_dsa*). Para terminar, copiaremos la clave pública (*id_dsa.pub*) al directorio personal del usuario que se encuentra en el servidor, pero dentro de la carpeta *.ssh* (si continuamos con el ejemplo, la ruta completa del archivo sería *C:\users\Jose\id_dsa.pub*.

Por último, renombraremos este archivo en el servidor, pasándose a llamar *authorized_keys2*. Concluiremos reiniciando el servicio y, cuando accedamos al servidor de nuevo, no será necesario introducir contraseña alguna ya que se utilizarán automáticamente las claves públicas y privadas generadas anteriormente.

9 Eliminar SFTP y SCP

Intermedio



9

Está claro que estos dos servicios deben sólo ofrecerse en aquellas cuentas que ofrezcan una confianza plena. Por esto mismo, en el resto será más que conveniente eliminar la posibilidad de que se efectúen este tipo de conexiones. Para ello abriremos el fichero *passwd* y sustituiremos el último parámetro (normalmente */ssh/switch*) por */ssh/quietcmd*.

10 Reenvío de puertos: un VNC cifrado

Avanzado

Si existe alguna característica que pruebe la flexibilidad de SSH, esa es el reenvío de puertos cifrado. Aunque sus posibilidades son mucho más amplias de lo que aquí comentaremos, básicamente consiste en crear una conexión entre dos equipos que será utilizada por otro programa (sin saberlo) para comunicarse. Pero se entenderá mejor con un ejemplo de gran utilidad. Utilizaremos en esta ocasión un pequeño programa de control remoto desarrollado por los laboratorio de AT&T llamado VNC (*www.uk.research.att.com/vnc*). Esta herramienta destaca por su sencillez de uso y disponibilidad en la mayoría de las plataformas. Consiste en un cliente y un servidor que se comunican entre sí utilizando el puerto 5900 (al menos en la plataforma Windows). La única desventaja radica en la debilidad de sus contraseñas por lo que no es conveniente la instalación de un servidor WinVNC en un equipo cualquiera.

Utilizando SSH haremos que el canal de comunicación entre el servidor VNC y su cliente esté completamente cifrado, incluso antes de introducir la contraseña. Para esto será necesario que el equipo que vamos a controlar disponga de un servicio OpenSSH instalado y configurado. Una vez hecho esto, modificaremos las siguientes claves del registro (creándolas si es necesario tanto en el servidor como en el cliente):

[HKEY_LOCAL_Machina\SOFTWARE\ORL\WinVNC3]
«AllowLoopback»=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3\Default]
«AllowLoopback»=dword:00000001

Hecho esto, en el equipo cliente abriremos una línea de comando y teclearemos lo siguiente: *ssh -N -C -L 5900:servidor:5900 servidor*. Con la opción *–N* evitaremos que SSH abra una línea de comandos, con *-C* que la transmisión además de cifrada se comprima y *-L* permite redirigir los puertos (el puerto 5900 en nuestro equipo local es redirigido al 5900 del equipo remoto).

Hecho esto, abriremos el cliente y, cuando nos pida introducir el servidor, teclearemos *localhost* (seguido del puerto que hayamos configurado, normalmente 0, quedando de esta forma: *localhost:0*).

11 VPN con PGPi

Intermedio

Una de las herramientas que se ha hecho famosa por mérito propio es PGP. Su versión internacional y gratuita también permite el cifrado de las comunicaciones. En concreto podremos establecer una completa VPN, independientemente del sistema operativo de que dispongamos, ya que el programa está disponible para casi todas las versiones de Windows. La instalación del programa no nos supondrá problema alguno; sólo tendremos que acordarnos de señalar la copia del módulo PGPnet. Tras esto, será necesario que creemos un nuevo par de claves publica/privada, con las precauciones habituales.

Hecho esto, se instalará un módulo que, a modo de tarjeta de red, será el verdadero encargado de evitar todo posible espía en el camino de nuestros datos. PGPnet permite utilizar cifrado de comunicaciones de un equipo a otro o entre grupos de equipos. En ambos casos, la configuración es muy similar.

Tras la instalación del programa nos dirigiremos al icono que aparece en la parte inferior derecha con forma de candado. Pulsaremos con el botón derecho, seleccionaremos la opción *PGPnet* y *VPN*. En la ventana que aparece, bajo la pestaña *VPN* seleccionaremos *Añadir*. Un pequeño asistente aparecerá y nos guiará a través de los datos necesarios. Básicamente tendremos que introducir la dirección IP (o nombre) de aquellos equipos con los que queramos comunicarnos de forma segura. Si introducimos una subred completa, todas nuestras comunicaciones serán inviolables, al menos de forma teórica.



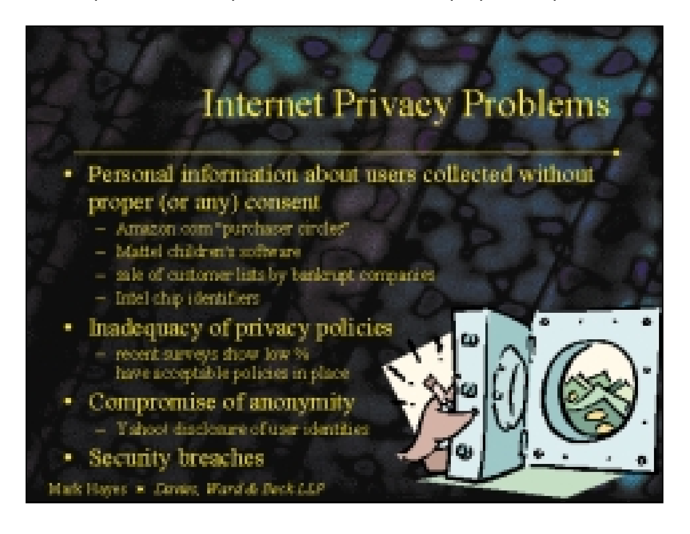
Recursos de anonimato en Internet

Información, consejos y utilidades para navegar de forma anónima


A la hora de navegar a través de Internet o utilizar nuestro correo electrónico, corremos una serie de riesgos que nos pueden ocasionar graves problemas. Nos referimos al espionaje por parte de agentes externos a nuestro sistema, lo cual representa una clara violación de la intimidad.

Para ello existen diferentes utilidades y programas que pueden evitar, al menos durante un tiempo, que suframos este tipo de «violaciones». De todos modos, también hay multitud de usuarios que desconocen por completo los riesgos que esto supone y que tampoco saben cómo solucionarlo en el caso de sufrirlo. Por esta misma razón, en la propia Red se pueden encontrar muchas páginas web disponibles para cualquier usuario y que les ayudarán en estas labores a través de artículos e informes explicativos acerca de temas como el anonimato en la red, la encriptación de datos, etc. Asimismo, en gran parte de las mismas existen accesos a diversos foros y grupos de noticias, que nos servirán de gran ayuda ya que, de este modo, tendremos la opinión, ayuda y consejos de personas que hayan sufrido ataques de este tipo o de cómo se han preparado para recibirlos y paliarlos. Una vez pensemos que estamos advertidos acerca de los peligros que corremos en la navegación por la Web, ya estaremos preparados para elegir el tipo de software que más nos interesa para, de este modo, proteger nuestro equipo de intrusos no deseados y poder navegar de un modo totalmente anónimo.





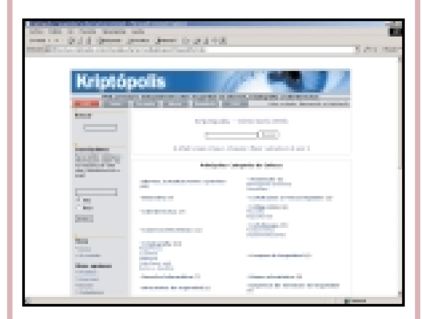


Para ello, en las próximas páginas os exponemos algunos ejemplos de *sites* relacionados con estos temas así como una descripción de los servicios que cada uno de ellos nos ofrece. Encontraréis un total de seis ejemplos en los que hemos procurado cubrir todos los aspectos relativos a temas que os puedan interesar relacionados con la navegación anónima.

Estamos seguros de que os serán de gran ayuda para evitar muchos de los problemas derivados de la navegación por la Red.







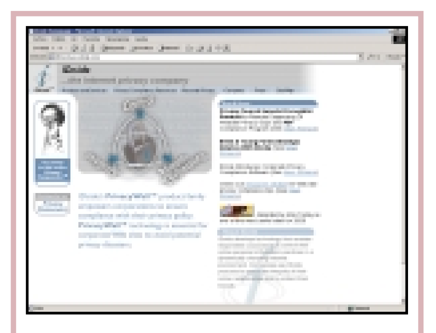
Kriptopolis

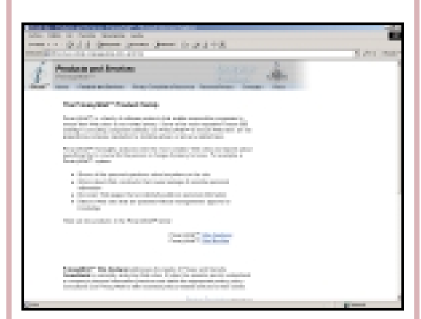
www.kriptopolis.com/

Esta web está dedicada a aquellos usuarios interesados en aspectos tales como seguridad en Internet, criptografía o ciberderechos. Incluye gran cantidad de noticias y eventos relacionados que se van actualizando día a día aunque, para no tener que visitar la web, tenemos la posibilidad de suscribirnos de forma que recibamos la información periódicamente por medio de correo electrónico. Asimismo, encontraremos *links* que nos acercarán al mundo de los *hackers* y la criptografía por medio de diferentes documentos e informes escritos por especialistas en el tema.

Una de las áreas más llamativas de este *site* es aquella conocida como de descarga. En este apartado encontraremos multitud de utilidades y pequeños programas relacionados con estos temas. Vienen distribuidos por categorías entre las que podemos destacar una de antivirus, protección y desprotección de sistemas, privacidad y *anticookies*, cortafuegos o detección de intrusos.

También encontraremos un apartado de enlaces a otras páginas relacionadas con diferentes temas como anonimato, criptografía, privacidad o protección de contenidos entre otros muchos. Para terminar comentaremos que todos los amantes de estos temas hallarán gran cantidad de información y cuentan con la ventaja de que todos los contenidos expuestos vienen en castellano.





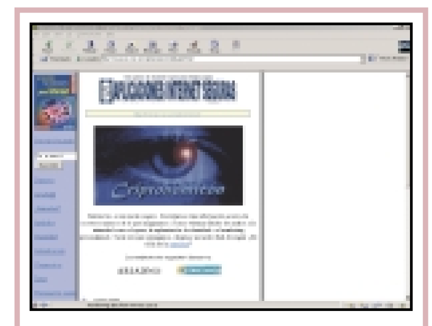
IDcide

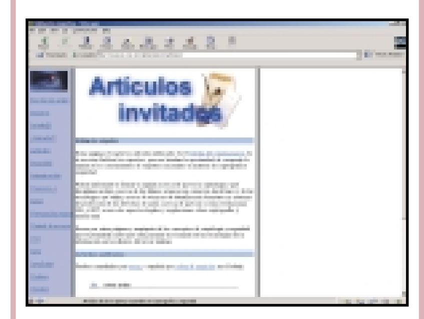
www.idcide.com/

Esta es una página web que, como principal característica, cuenta con una herramienta que servirá al usuario de ayuda a la hora de asegurar su privacidad mientras navega de manera convencional a través de Internet. Una vez conectados a este *site*, podremos descargarnos el mencionado programa y de modo completamente gratuito. Una vez lo hemos descargado e instalado, el internauta sabe si la visita que está realizando a una determinada página está siendo seguida por empresas publicitarias o de marketing.

En la misma página se recogen una serie de *links* que nos llevarán hacia otros portales relacionados con la privacidad y el anonimato en Internet. Tal y como es habitual en estas páginas, también cuenta con un área de noticias en la que encontraremos todas las novedades acaecidas en el mundo y relacionadas con la privacidad en la Red.

Para aquellos que no estéis demasiado familiarizados con estos temas, podéis encontrar un completo glosario de términos específicos que os ayudarán a comprender en qué consiste y cómo os puede ayudar el anonimato en la red. Eso sí, quizá para algunos de vosotros resulte un inconveniente el hecho de que este *site* esté en inglés. Asimismo los expertos encontrarán su sitio en el apartado de trucos en el que los usuarios van dejando sus sugerencias y «triquiñuelas».





Criptonomicón

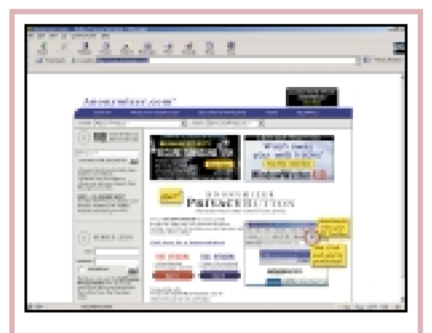
www.iec.csic.es/criptonomicon/

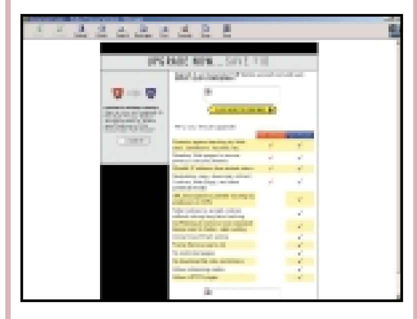
Esta es una página en castellano en la que encontraremos una amplia información acerca de los temas más candentes sobre la privacidad y anonimato en la red. En cada uno de los apartados disponibles contamos con información sobre el tema con ejemplos, demos y consejos para que la navegación pueda resultar más segura para cualquier persona, y todo ello de la manera más sencilla posible.

Este *site* también cuenta con su propio apartado de artículos relacionados con el tema. Éstos servirán de gran ayuda a aquellas personas que se estén introduciendo en estas labores, ya que han sido realizados por verdaderos expertos.

Entre los diferentes apartados con los que contamos, podemos destacar aquellos relacionados con la seguridad, autenticación, comercio electrónico, *cookies*, anonimato, correo y navegación seguras, etc. En la mayoría de ellos, cuando nos ponen ejemplos prácticos, vienen divididos por el tipo de navegador que se utilice en cada caso, es decir, Netscape o Explorer. El *site* también incluye dos útiles *links* dedicados a las aplicaciones realizadas con Java y JavaScript, donde podremos encontrar diferentes consejos y aplicaciones relacionadas con la seguridad.

Para los amantes de los temas de seguridad, esta es una web que servirá de gran ayuda para infomarnos acerca de los aspectos más oscuros de este mundo de la criptografía.

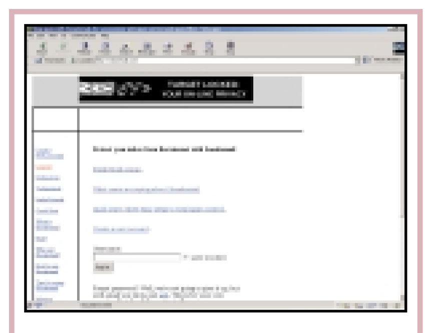


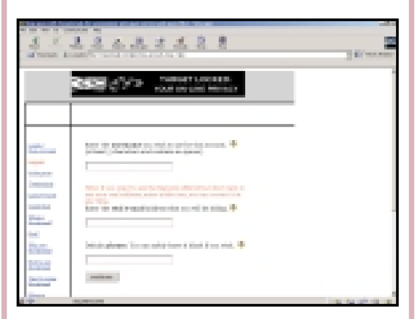


Anonymizer

www.anonymizer.com/

Esta es una página especialmente enfocada al anonimato en Internet. En ella podremos encontrar multitud de utilidades y servicios relacionados con este tema. Fundamentalmente se centran en proporcionar a los usuarios diferentes herramientas y productos software que podemos descargar, ya sea de manera gratuita o por medio de pago. Para encontrarlos fácilmente, estos programas están ordenados por diferentes categorías y temas. Entre ellas podemos mencionar la navegación anónima, *bookmark* privados, etc. Asimismo, en la página de inicio encontramos un programa llamado Anonymizer PrivacyButton, válido para navegar por la Red con Internet Explorer de Microsoft. En realidad se trata de una herramienta de seguridad, de modo que, cuando utilicemos este navegador, la conexión sea anónima. Eso sí, previamente nos tendremos que registrar en la página con el fin de conseguir nuestro propio nombre de usuario y *login* para la posterior descarga. También en otro de los apartados del *site* encontramos un departamento con las noticias más recientes además de opiniones de otros usuarios acerca del programa anteriormente mencionado. Esta página está especialmente diseñada para aquellos usuarios que desconfíen de su conexión a Internet y deseen estar protegidos contra agentes externos y *hackers*. La página en su totalidad se encuentra en inglés.



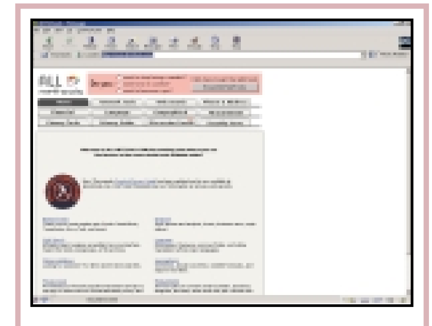


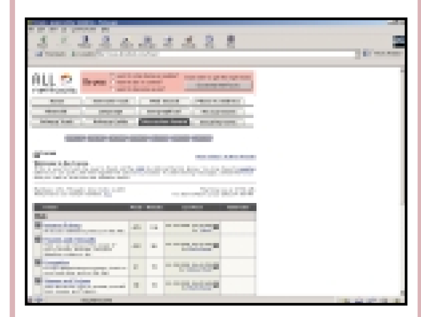
Sneakemail

http://sneakemail.com/

Esta página está especialmente diseñada para aquellos usuarios que desean contar con un total anonimato a la hora de utilizar el correo electrónico convencional. Se trata de un servicio gratuito desde el que podremos crear cuentas de correo ficticias, es decir, se trata de crear un alias a partir de una cuenta real que ya tengamos dada de alta previamente. Estas cuentas pueden utilizarse en formularios de la Web y, de este modo, gracias al anonimato que nos proporciona, evitar recibir correo no deseado en la cuenta real anteriormente mencionada. En la página, que se encuentra en inglés, además del mencionado servicio encontraremos amplia información acerca de por qué nos puede ser de utilidad además de cómo utilizarlo. Para aquellos que no estéis familiarizados con el tema, también encontraréis explicado el modo de utilización así como los perjuicios que nos puede ocasionar el no funcionar con este servicio en determinados casos.

Dar de alta la utilidad resulta muy sencillo, ya que en la página principal encontraremos un *link* llamado *Create a new account* en el que posteriormente se nos solicitará el nombre de nuestra cuenta real así como el alias que deseamos darle. Encontramos además un apartado en el que se incluyen diversos enlaces a otras páginas que traten temas del mismo tipo.





All:nettools

www.all-nettools.com/privacy/

Todos los temas relacionados con la encriptación de datos en Internet no son conocidos por todo el mundo y precisamente aquellas personas que no entiendan demasiado de estos temas pueden utilizar este *site* como método informativo y de aprendizaje. Esta página supone una excelente y actualizada guía *on-line* en la que podemos encontrar diversos consejos prácticos sobre temas como la privacidad en Internet, el anonimato, cifrado, cortafuegos, etc.

En todos los apartados que os hemos mencionado tendréis disponibles una gran cantidad de artículos y estudios clasificados por temas. Estos incluyen capturas demostrativas y explicaciones de cómo proteger nuestra máquina ante agentes externos cuando navegamos por Internet. Además, entre las diferentes utilidades incluidas, se encuentra un foro donde los usuarios dan diferentes opiniones y consejos, un enlace a las últimas noticias relacionadas con la seguridad y el anonimato, algún software útil para estos menesteres así como un buscador de la Web. A modo de utilidad curiosa cabe comentar que también disponemos de diferentes conversores de medidas de longitud, de horas del mundo y de dominios. El único problema (para algunos usuarios) que este *site* os puede presentar, es que toda la información y contenidos se encuentran en inglés.



Chatarra informática

Aprovechar equipos antiguos con sistemas operativos como Linux

Avanzado

Durante el paso de los años, mucha gente ha ido acumulando piezas y piezas de equipos que antes eran de última generación y que ahora se ha convertido en «tecnochatarra». La mayoría, antes o después se encuentran con auténticos arsenales de placas base antiguas, procesadores desfasados y discos duros de tamaño ridículo. Habitualmente, nuestro desguace acaba ocupando mucho más espacio en nuestro lugar de trabajo que el equipo que utilizamos, con el agravante de que a estos últimos vestigios no le sacamos partido alguno. Existe sin embargo una forma de aprovechar todos estos recursos aparentemente inservibles. Consiste en crear un cluster de equipos. Utilizando estos sistemas conseguiremos que varios equipos actúen de forma coordinada, distribuyéndose la carga de trabajo entre ellos.

En nuestro haber contábamos con dos equipos de similares características: dos Pentium 166 MHz con discos duros de 2 Gbytes, 40 y 64 Mbytes de RAM, tarjeta gráfica integrada en placa (ATI Mach 64 CT) y controladores IDE. Además, un equipo bastante más potente servirá de coordinador en la distribución del sistema operativo, algo que, como ya veremos, simplificará mucho la instalación de Linux en los clientes. Puede que, con dos únicos «nodos» en nuestro cluster, esta ventaja puede pasar desapercibida; sin embargo, será de gran utilidad para aquellos que se dispongan a montar un número superior de equipos. Este último equipo era un Pentium II 500, con 8 Gbytes de disco duro y 128 Mbytes de RAM.

Necesitábamos además tarjetas de red para todos ellos, para lo que escogimos varias tarjetas de bajo coste y fáciles de encontrar: Realtek 129. Además precisamos de una unidad lectora de CD, con el fin de acelerar el proceso de instalación de uno de los clientes, para lo que tomamos prestada la unidad del servidor una vez estuvo preparado.

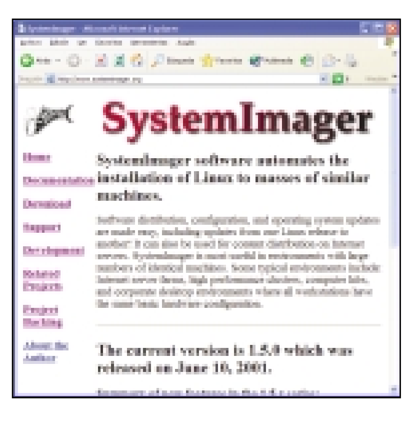
En primer lugar, creamos la infraestructura necesaria para que no tengamos que instalar y configurar todos los equipos. Para esto utilizaremos SystemImager, una aplicación que permite, entre otras cosas, crear una imagen de un equipo ya configurado, almacenarla en el servidor y distribuirla a todos los nodos, modificando tan sólo las partes que deban cambiar, como por ejemplo la dirección IP o el nombre del *host*. Pero, antes de comenzar, será necesario que instalemos este servicio en el equipo «coordinador».

El servicio SystemImager

Paso 1

El servidor SystemImager

Como ya hemos dicho, primero tendremos que instalar el servidor de SystemImager. En nuestro pequeño equipo «coordinador» disponíamos de Red Hat 7.2, además de cerca de 2 Gbytes de espacio libre para almacenar las imágenes de los clientes. Para comenzar, será necesario que descarguemos SystemImager y todos los paquetes que éste necesita para funcionar, es decir, *nasm*, *syslinux* y *rsync*, algunos de los cuales ya estaban instalados en nuestra distribución. Encontraremos una versión de cada uno de estos en *http://systemimager.org/download*. Tras descargar los archivos principales del servicio y descomprimirlos (*bzcat va-systemimager-server-x.x.x.tar.bz2 | tar –x*), tenemos que instalar el paquete (*./install*).



Paso 2

Asignar IP a los nodos

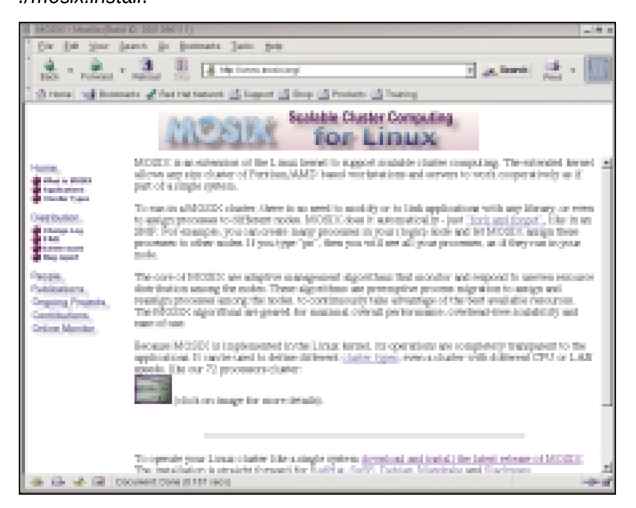
Aunque SystemImager permite asignar direcciones estáticas a cada uno de los equipos que posteriormente compondrán nuestro cluster, es mucho más interesante que éstas se asignen utilizando DHCP. La propia herramienta cuenta con un

pequeño *script* que nos guiará a lo largo del proceso de configuración del servicio llamado *makedhcpserver*. Hemos de introducir los datos habituales como el rango de direcciones disponibles para asignar, IP del servidor, DNS y otros parámetros. En nuestro caso, basta con completar el nombre del dominio, dejando el resto de los parámetros en sus valores por defecto.

El cliente de Oro

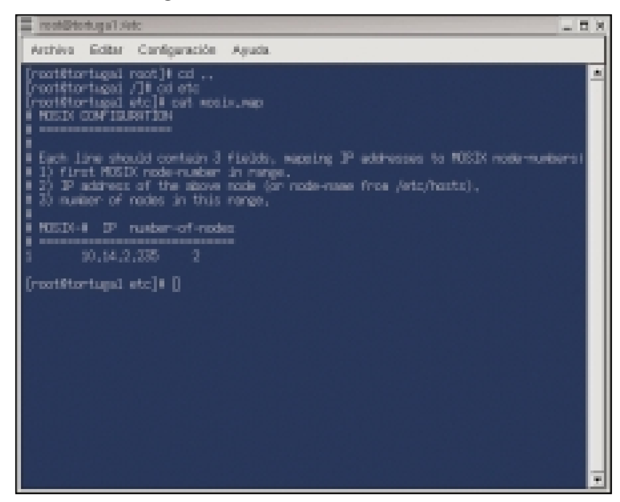
Paso 3
Crear el cliente base

En este punto nos dirigimos a uno de los ordenadores que actuarán como nodos del cluster. Este equipo lo denominaremos el «cliente de oro», ya que será el que configuraremos y cuya imagen se copiará al resto. En este caso, utilizamos también Red Hat 7.2, aunque sin algunos paquetes, ya que su disco duro (2 Gbytes) no da para mucho. Tras la instalación del sistema operativo, copiamos al directorio */usr/src* los fuentes del *kernel* 2.4.13 y el *tarball* de MOSIX (versión 1.5.2). Encontraremos estos archivos en *www.kernel.org* y *www.mosix.org*. Es muy importante que descarguemos los fuentes del núcleo directamente desde este repositorio ya que, de otra forma, puede que Mosix se niegue a instalar. Para comenzar con el proceso, descomprimiremos el archivo (*tar xzf MOSIX-1.5.2.tar.gz*) y dentro del directorio que crea ejecutaremos *./mosix.install*.



Comenzará preguntándonos dónde se encuentran los fuentes del *kernel*, que será necesario descomprimir. El resto de preguntas propias de Mosix fueron contestadas, al menos en nuestro caso, con las opciones por defecto. Automáticamente, el *script* nos mostrará la pantalla de configuración del *kernel*, paso previo antes de compilarlo. Dependiendo del hardware de nuestras máquinas, lo prepararemos de una forma u otra, aunque debemos ser precavidos ya que el mismo núcleo se ejecutará en todas ellas, y no conviene crear incompatibilidades. Aunque el proceso debería ser bastante sencillo, hemos de tener en cuenta una serie de factores antes de lanzarnos a compilar. Es muy recomendable que nuestra distribución esté soportada por Mosix, ya que éste realiza multitud de cambios de forma automática en los *scripts* de inicio. Dado que éstos generalmente varían de una distribución a otra, y modificar todos los ficheros que lanzan un «demonio» es una tarea en ocasiones abrumadora, conviene asegurarnos con anterioridad. En el caso contrario, en el fichero README incluido aparecen todos los pasos a seguir de forma manual. Otro fallo más que probablemente viene dado por la falta de paquetes necesarios para compilar el *kernel*. Si nos encontramos en esta situación, será necesario que realicemos la compilación en otro equipo y copiemos posteriormente la imagen y sus módulos al equipo que luego formará un nodo del cluster. Pero, dado que no nos interesa modificar todos los ficheros de configuración de forma manual, tendremos que recurrir a los *scripts* que se encuentran en el directorio *inst* creado al descomprimir Mosix. Éstos permiten desde la instalación de los manuales hasta la modificación de los ficheros de inicio.

Paso 4
La configuración de cluster

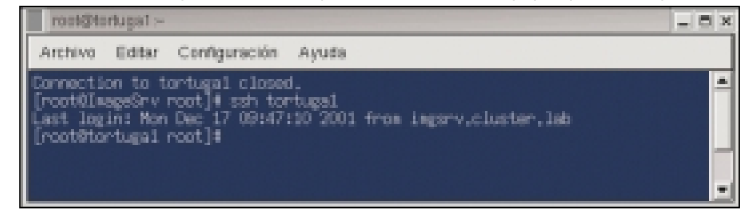


Antes de arrancar el equipo, conviene que editemos un par de ficheros que emplea Mosix para su configuración. En primer lugar, es necesario modificar */etc/mosix.map*. Éste determina las máquinas que forman parte de un cluster. Cada línea en el fichero, que representa un grupo, debe tener tres campos: el primero, un identificador del grupo, el segundo, la dirección IP del primer nodo y, para terminar, el número de nodos. Este fichero debe ser coherente entre todos los participantes del grupo, sin embargo, ya que vamos a efectuar una imagen de este equipo, esto no será un problema.

A continuación debemos modificar el fichero *rc.local* e incluir una línea similar a esta: *mosctl setyard P/166*. Esto le indica a Mosix que la máquina en la que se está ejecutando nada tiene que ver con un Pentium III a 1.000 MHz, y que debe ajustarse a unas medidas algo inferiores.

Paso 5
Seguridad sin contraseña

Antes de crear la imagen, conviene que pensemos en el programa de administración y sus requerimientos. Existen diversas aplicaciones, pero sin duda MosixView es la más llamativa. La única dependencia que la herramienta nos impone es que debe ser capaz de entrar en el equipo que forma parte del

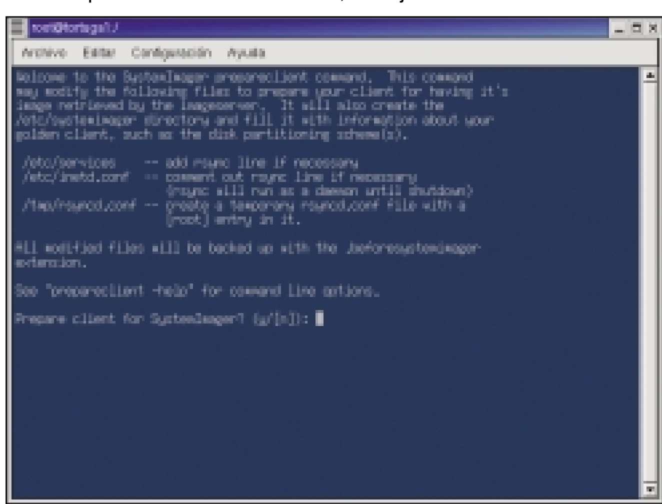


cluster sin introducir clave alguna, ya sea utilizando *rsh* o *ssh*. De una forma u otra, vamos a tener que configurar el equipo; lo haremos con este último, ya que añade seguridad a todo el conjunto. Para esto nos dirigiremos al equipo desde el que vamos a administrar el cluster. En éste, que en nuestro caso también se trata del servidor de imágenes, comenzaremos verificando si el servicio *sshd* está en marcha. Para ello, ejecutaremos */etc/init.d/ssh Status* y, en el caso que esté detenido, lo arrancaremos (*/etc/init.d/ssh Status*). Hecho esto, tenemos que crear el par de clave pública/privada que servirán de base para la autenticación sin contraseña. Para ello, nos dirigiremos al directorio */root* y allí crearemos un subdirectorio llamado *.ssh*. Desde este último, llamaremos a la aplicación *ssh-keygen* (con el parámetro *-t rsa*), quien se encargará de generar estas claves. A continuación, copiaremos el fichero denominado *rsa_id.pub* (o *identity.pub*) para que exista un nuevo fichero llamado *authorized_keys2*. Este fichero también lo copiaremos en el directorio */root/.ssh*, que crearemos si no existe, del «cliente de oro». Para concluir, tendremos que añadir la líneas *eval ssh-agent* y *ssh-add* a nuestro fichero de login (*/root/.bashrc*).

Paso 6

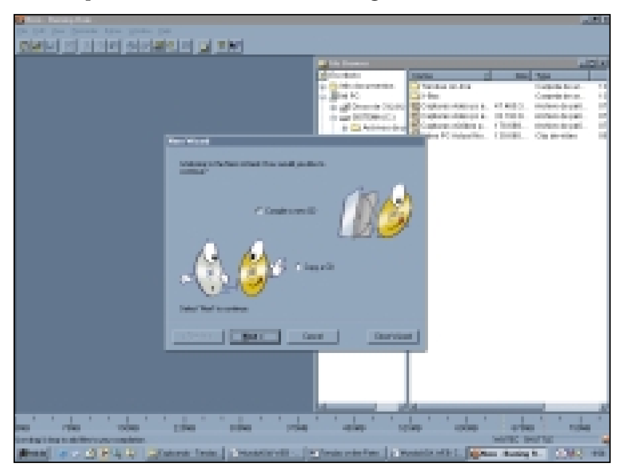
Creación de la imagen

Por fin estamos en disposición de crear la imagen que definirá el resto de los clientes. Para ello, descargaremos el paquete que se encuentra en la página web de SystemImager: *systemimager-client-1.5.0.tar.bz2*. A continuación, lo descomprimiremos e instalaremos con el simple *script* que dispone para ello. Es conveniente que antes de esto nos hayamos asegurado que nuestro servidor de imágenes es también el servidor DHCP del cluster. Para preparar la imagen, tras la instalación ejecutaremos en el cliente *prepareimage*. El comando se encargará de crear un listado con las particiones a almacenar en el fichero. Pero realmente, para crear este archivo nos dirigiremos al servidor, donde ejecutaremos *getimage*. Esta herramienta, a la que debe proseguir el parámetro *-golden-client* y el nombre del cliente y *-image* y el nombre de la imagen, es el que verdaderamente generará la copia utilizando para ello el «demonio» *rsync* instalado en el cliente.
Tras la larga copia, será necesario que configuremos la imagen. Para ello tendremos que elegir, en primer lugar, el mecanismo que seguiremos para asignar direcciones IP a los clientes. Disponemos de cuatro opciones, pero ya que tenemos preparado el servidor DHCP utilizaremos esta opción como método preferente. A continuación, se ejecutará de forma automática el programa addclients. Éste configurará el nombre de cada uno de los clientes de forma automática en los ficheros /etc/host de las imágenes.



Paso 7

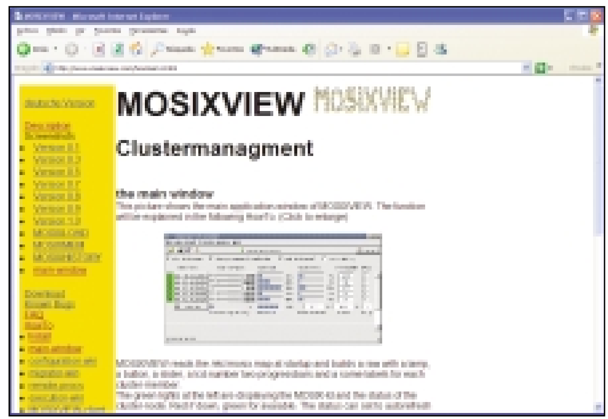
Duplicación de las imágenes



A partir de este momento, añadir nuevos nodos a nuestro cluster es pan comido. Tan sólo hemos de descargar de *www.systemimager.com* una pequeña imagen *iso* que ocupa 2 Mbytes. Con ésta hemos de arrancar el siguiente nodo, para lo cual tenemos que haber grabado el fichero en un CD-ROM previamente. Tras iniciarse, el equipo buscará mediante DHCP el servidor de imágenes y comenzará con la transferencia e instalación de forma completamente automática.

Paso 8

Administración de tareas



De aquí en adelante, podemos escoger múltiples opciones de administración, desde las herramientas incluidas con el propio Mosix u otras que harán la monitorización del sistema completo mucho más sencilla. Hemos de advertir que tendremos que ser bastante diestros a la hora de manejarnos entre *displays* remotos, *ssh* y otras herramientas de Unix típicas de sistemas «multi-equipo», por lo que un buen vistazo al manual nunca estará de más. Como última recomendación os recomendamos la página de MosixView, un programa externo que nos ayudará, cuando nos hayamos hecho con él, a ver más claramente el funcionamiento de este completísimo método de aprovechar hasta el último recurso.

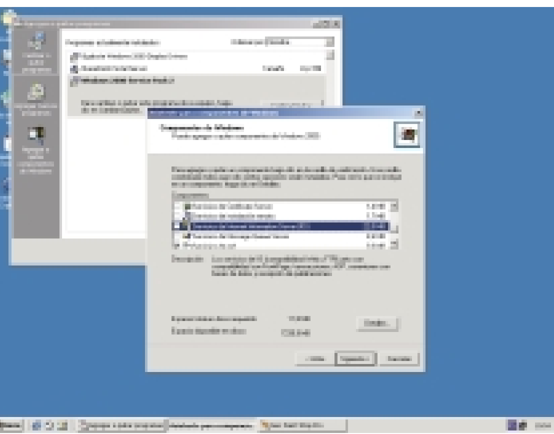


Intranet corporativa

Poner a punto una red empresarial

Avanzado

Ahora es más sencillo que nunca montar una buena infraestructura informática profesional. Con un poco de paciencia y ganas de aprender será posible hacer el montaje. Vivimos en una nueva etapa de la informática, en la que todo gira en torno a la comunicación en red y donde, a través de este mismo medio, es posible realizar infinitas tareas que antes casi parecían imposibles. En las páginas siguientes vamos a contar algunas de las muchas posibilidades a las que podemos acceder con los ordenadores de nuestra compañía conectados en red. Partimos de la base de que contamos con un servidor de potencia media (Pentium III en adelante), una buena cantidad de memoria (mínimo 256 Mbytes, recomendable 512 Mbytes) y unos buenos discos duros de unos cuantos «gigas». En el número anterior de este mismo Manual de Trucos & Utilidades Internet ya hablamos de cómo poner en marcha un servidor con Windows 2000 Server, configurarlo como controlador de dominio y crear los diferentes usuarios que podrán acceder a la red desde cada uno de los puestos de la misma. Tomando como base esta plataforma, seguiremos complementando las posibilidades de nuestro servidor, añadiéndole funciones adicionales. Así, instalaremos en él nuestra página web corporativa, desde la que podremos informar a los empleados de los diversos eventos de la compañía, intercambiar información entre departamentos o dejar disponibles *on-line* archivos y documentos que puedan ser necesarios para el trabajo del día a día. Por supuesto, hablaremos de los posibles entornos con los que podremos crear esta página web residente en nuestro servidor y accesible desde cualquiera de los ordenadores de nuestra red.



Por otra parte, también veremos cómo instalar una máquina dedicada en exclusiva a las copias de seguridad, apoyándose en diversas medidas de seguridad hardware y software para impedir la pérdida de datos o el acceso no autorizado a los mismos. También trataremos de explicar la manera de instalar un antivirus en red, capaz de actualizarse automáticamente vía Internet. Por último, hablaremos de la forma de inventariar convenientemente toda nuestra infraestructura informática y documentar todos y cada uno de los aspectos de la misma.

Primeros pasos en el sistema Windows 2000 Server

Como ya hemos comentado, partimos del supuesto de que ya tenemos Windows 2000 Server instalado y funcionando. Habremos configurado nuestro servidor como controlador principal de dominio, al tiempo que tendremos creados y ajustados cada uno de los usuarios del mismo. Ahora bien, uno de los pilares fundamentales para poder llevar a cabo la mayor parte de las tareas que veremos en las páginas siguientes será la instalación del *Internet Information Server*, también conocido como IIS. Este paquete incluye toda una serie de servicios que habilitarán la máquina como servidor web, FTP, además de otras funcionalidades necesarias para desempeñar estas tareas.

Es muy probable que no se encuentre instalado en nuestro sistema. Para ello, acudiremos a *Inicio/Panel de Control/Agregar o quitar programas/Agregar o quitar componentes de Windows*. En la nueva ventana aparecerá una lista de componentes y, al final de la misma, buscaremos uno llamado *Servicios de Internet Information Server* (IIS), tal y como podéis ver en la imagen 1. Si ya está marcado, será indicativo de que ya se encuentra instalado. De lo contrario, haremos clic sobre su casilla de verificación para indicar su instalación. Si además pinchamos sobre *Detalles*, podremos decidir qué componentes específicos se instalarán, aunque los indicados por defecto son suficientes. Tras esto pulsaremos *Siguiente*, tras lo que se nos pedirá el CD-ROM de instalación y se configurará todo el servidor. Esta tarea llevará unos cuantos minutos, dependiendo de la potencia de la máquina. Ahora sí estamos listos para empezar a construir nuestra propia Intranet corporativa.



Paginas Web en red

Poner en marcha el servicio web

Intermedio

Antes de hablar sobre la manera en la que tendremos que llevar a cabo la configuración y ajuste de nuestro servidor web, comentaremos algunas cosas relacionadas con este tema. Lo primero, y muy importante, es que para los siguientes pasos hemos utilizado como plataforma común Windows 2000 Server. Bajo este sistema operativo resulta sencillo poner en marcha un auténtico servidor de páginas web sin grandes complicaciones, asequible para los menos expertos. Por supuesto, hay opciones mucho más económicas como el conocido Apache que corre bajo Linux y su coste es sencillamente cero. Sin embargo, tendremos que tener conocimientos avanzados sobre instalación y administración de este sistema operativo. Por el contrario, bajo Windows 2000 Server nos encontraremos con una interfaz muy similar a la que habitualmente estamos utilizando y unas enormes posibilidades una vez que buceemos un poco entre el maremagnum de posibilidades.

El segundo aspecto que tendremos que tener en cuenta es que sería conveniente y útil instalar en la máquina el servidor DNS, gracias al cual podremos resolver fácilmente el nombre de una máquina de la red sin saber su dirección IP. Esto se puede hacer automáticamente en el momento de crear el controlador de dominio ya que, en caso de existir un servidor DNS en nuestra red, nos da la opción de instalarlo.

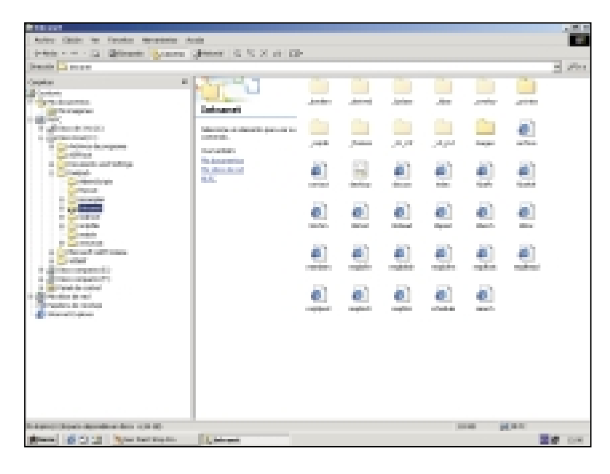
Por otra parte, y como ya hemos comentado en otras páginas, damos por hecho que ya tenemos instalado un controlador de dominio (que puede ser esta misma máquina), y que contamos con la red perfectamente configurada. Además, en la página anterior ya hemos hablado sobre la manera de instalar el IIS (*Internet Information Server*), componente necesario para que funcionen cada uno de los apartados que tratamos en estas páginas. Por último, suponemos que también tendremos creado el sitio web de nuestra intranet. En caso de que os surjan dudas al respecto, más adelante trataremos de manera superficial las distintas posibilidades que tenemos a la hora de crear nuestro sitio web.

Dicho todo esto, vamos a ver cómo configurar nuestro servidor para que sea capaz de servir (valga la redundancia) páginas web al resto de máquinas que forman parte de nuestra red.

Paso 1

Ubicar el sitio web

Una vez tengamos instalado el IIS en nuestro servidor, hemos de empezar a seguir los pasos para hacer accesible nuestras páginas HTML. Lo primero que haremos será crear un directorio en el que guardaremos todo el sitio web al completo. Salvo que nuestras preferencias indiquen lo contrario, lo más sencillo es crear un subdirectorio en la carpeta *Inetpub*, que por defecto cuelga de C:. En nuestro caso hemos creado un directorio llamado *Intranet*, dentro del que hemos guardado todos los archivos que componen nuestro *site*. Aquí incluiremos las páginas HTML, los gráficos y demás componentes que requieran nuestra estructura.

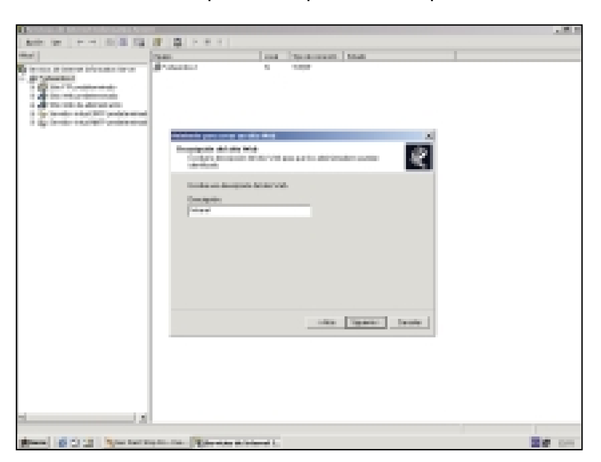


Paso 2

Crear un sitio web

A continuación vamos a crear un nuevo sitio en nuestra consola de administración de los servicios de Internet. Para ello, iremos a *Inicio/Programas/Herramientas administrativas/Administrador de servicios Internet*. Aparecerá una ventana en la que podremos ver cada uno de los apartados que gestiona esta consola. Si hacemos clic con el botón derecho del ratón sobre el nombre del servidor, raíz de toda la estructura, aparece un menú contextual. En él seleccionaremos la opción *Nuevo/Sitio Web*.

A continuación arrancará un sencillo asistente que nos pedirá el nombre del sitio primero. Aparecerá después una nueva



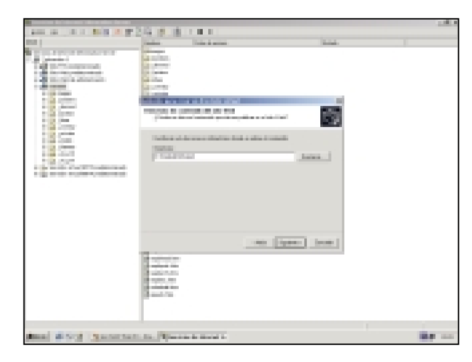
pantalla en la que indicaremos algunos parámetros que podremos dejar por defecto y, por último, la ruta de búsqueda del sitio, en nuestro caso *C:\inetpub\Intranet*. Por último, veremos el nuevo sitio web en la columna de la izquierda.

Paso 3
Página de inicio

Cabe la posibilidad de que nos aparezca la web con la palabra *detenido*. Una de las causas del problema puede residir en el nombre de nuestra página de inicio. Para modificar este parámetro haremos clic con el botón derecho sobre el nombre del sitio web y seleccionaremos *Propiedades*. En la nueva ventana, repleta de opciones, acudiremos a la pestaña *Documentos*. Aquí veremos que se encuentran por defecto como páginas de inicio los archivos con nombre «Default». En caso de que nuestra página sea del tipo «index.htm», no tendremos más que pulsar *Agregar* e introducir el nombre exacto de la misma. Con las flechas de la parte izquierda podremos aumentar o reducir su prioridad de carga en caso de que existan de cada tipo especificado.
Hecho esto, pulsaremos *Aceptar*, de nuevo haremos clic con el botón derecho sobre el sitio web que hemos creado y pulsaremos sobre la opción *Iniciar*. Si todo esta correcto, la palabra *detenido* desaparecerá.

Paso 4
Directorio virtual

Uno de los últimos pasos para que todo funcione correctamente reside en crear un directorio virtual dentro del sitio web que hemos creado anteriormente. Haremos clic con el botón derecho sobre nuestro sitio y seleccionaremos la opción *Nuevo/Directorio virtual*. De nuevo aparecerá un pequeño asistente que nos pedirá el nombre del mismo y su ruta de búsqueda, donde especificaremos la misma que en el caso anterior. Por último, tendremos que decidir qué clase de operaciones se permitirán en él. Lo mejor es dejar las opciones marcadas por defecto.



Paso 5
Visitar la web

El último paso será comprobar que todo ha salido bien con lo que acudiremos a cualquiera de las máquinas de nuestro dominio y abriremos el *Explorador*. Podremos introducir la dirección IP seguida del nombre del directorio virtual en el cual alojamos nuestra web o, alternativamente, su nombre exacto seguido del mismo directorio virtual. Como ejemplo, en nuestra red utilizamos la ruta *http://192.168.0.1/intranet* o *http://servidor/intranet/* indistintamente. Al abrir esta dirección en el navegador de la máquina de la red, aparece ante nosotros la web alojada en el servidor.

A partir de este momento, las posibilidades de este servicio dependerán únicamente de nuestras capacidades desarrollando páginas web. Y es que podemos añadir capacidades para compartir ficheros vía FTP (en las páginas siguientes veremos cómo activar un servidor FTP), montar foros de discusión, agendas del día o informar sobre eventos y actos corporativos.



Servidor FTP

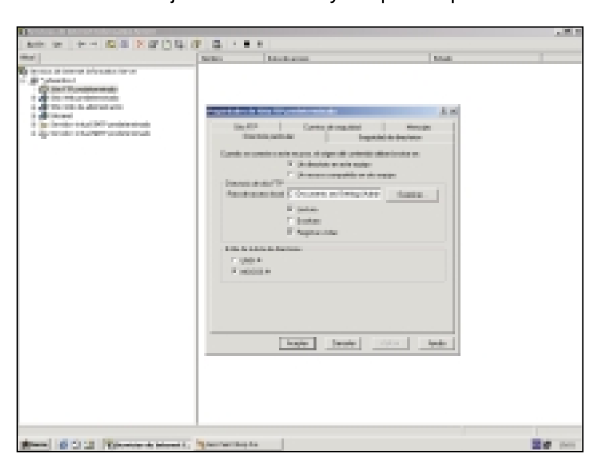
Transferencia de archivos vía red

Intermedio /

Ya sea para permitir la descarga de archivos como para enviar ficheros a un lugar determinado de nuestra red, con el protocolo FTP podremos disfrutar de toda clase de tareas con ficheros. Sin embargo, su uso es cada vez menor, y en entornos corporativos casi inexistente. La razón es que ahora resulta mucho más sencillo compartir carpetas y transferir ficheros desde el conocido *Entorno de red* de Windows. Ahora bien, en determinados momentos puede resultarnos tremendamente útil ya que, además de permitir un mayor control de acceso basado en usuarios y contraseñas, la velocidad de transferencia está bastante más optimizada. Además, puede resultarnos útil para compartir grandes librerías de datos con gran cantidad de ficheros. Esto sin olvidar que podremos apoyarnos en este servicio para descargar ficheros desde nuestra intranet corporativa. Y es que cualquier navegador moderno puede acceder a un sitio FTP para descargar ficheros. Dicho esto vamos a ver cómo, bajo Windows 2000 Server, podemos poner a punto este servicio que se basa en IIS.

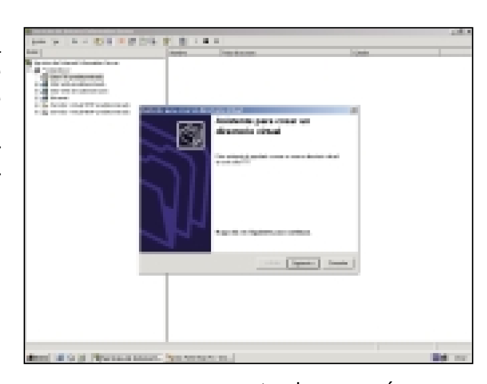
Paso 1
Puesta en marcha

Dado que ya tenemos instalado el IIS con su componente de servicio FTP, no tendremos que realizar instalaciones adicionales, sólo hemos de configurar el servicio. Para ello acudiremos a *Inicio/Programas/Herramientas administrativas/Administrador de servicios Internet*. En la ventana tendremos que dirigirnos a la columna izquierda, donde haremos clic con el botón derecho sobre *Sitio FTP predeterminado*. Dentro del menú seleccionaremos *Propiedades*, donde nos dirigiremos a las pestaña *Directorio particular*. En la casilla de *Ruta de acceso local* se especifica la ruta hacia la que actualmente se conectan los clientes por FTP (por defecto *\inetpub\ftproot*). Sin embargo, es posible cambiar esta ruta a la que más nos convenga, así como indicar si se podrá leer y/o escribir en ella. También resulta interesante la pestaña *Seguridad en directorios*, donde podremos indicar qué máquinas tendrán o no acceso a ciertos directorios. Igualmente, en *Mensajes*, escribiremos un mensaje de bienvenida y despedida personalizado.



Y bajo *Sitio FTP* indicaremos el máximo número de conexiones admitidas, mientras que en *Cuentas de seguridad* podremos decidir qué usuarios tendrán o no posibilidad de conectarse al servicio FTP. Una vez esté todo ajustado, simplemente pulsaremos *Aceptar*.

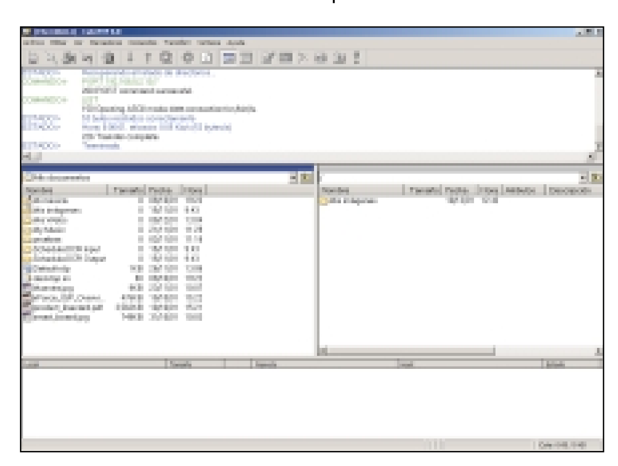
Paso 2
Directorio virtual



Ahora bien, no siempre querremos tener todos los archivos en el mismo emplazamiento. Para evitar esto se pueden crear los llamados *Directorios virtuales*, que crearemos haciendo clic con el botón derecho sobre *Sitio FTP predeterminado* y seleccionando *Nuevo/Directorio virtual*. Aparecerá uno asistente con el que le daremos un nombre e indicaremos la ruta de acceso. Gracias a esto, cuanto más tarde accedamos mediante un cliente de FTP, no tendremos más que cambiar a este directorio que, aparentemente, estará oculto a nuestra vista.

Paso 3
Acceso por FTP

Por último, podremos probar el funcionamiento del servidor FTP desde cualquier máquina conectada a nuestra red. Habrá que utilizar un cliente FTP para poder acceder, como por ejemplo el famoso CuteFTP (descargable desde *www.globalscape.com*) o el comando «ftp» de Windows NT/2000/XP. En cualquier caso, no tendremos más que especificar la dirección IP del servidor, indicar nuestro nombre de usuario y contraseña y comprobar que la conexión es correcta. De la misma manera, es posible probar a cambiar a alguno de los directorios virtuales mediante el comando correspondiente.





Documentos al estilo Web

Las ventajas de SharePoint Portal Server

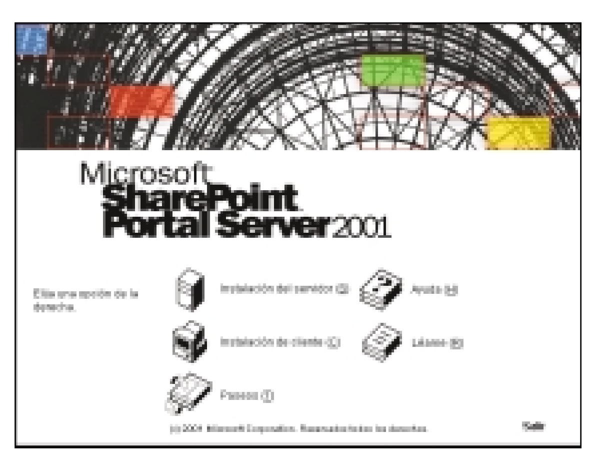
Avanzado

La mayoría de los entornos profesionales no aprovechan la integración del navegador o el sistema de ficheros de Windows. Toda esta potente integración la podemos ver en uno de los últimos lanzamientos de Microsoft. SharePoint Portal Server es un producto que bien puede haber pasado inadvertido ante el público general, sin embargo, propone un cambio radical en la metodología de trabajo. Gracias a él conseguiremos crear un portal de uso interno, evitando por otro lado largos tiempos de desarrollo e incluso la contratación de equipos externos que tan sólo compañías de tamaño mediano y grande pueden permitirse. Portal Server permite que hasta en las empresas con recursos limitados a un único administrador pueda gestionar una compleja infraestructura de trabajo. Decididos a sacarle el máximo partido a todas las aplicaciones de ofimática de las que disponemos, nos decidimos a instalar y configurar nuestro primer portal para controlar todo el proceso de creación de una pequeña sala de reuniones y tablón de anuncios desde donde los diversos departamentos se pueden comunicar. Además, esta comunicación no tiene por qué ser de «arriba abajo»; los empleados pueden utilizar áreas determinadas para anuncios menos formales.

Paso 1

La instalación

Comenzaremos con la instalación de la aplicación que exige unos requisitos bastante elevados. El servidor debe ejecutar Windows 2000 Server (o Windows 2000 Advanced Server), pero en éste no puede estar instalado Exchange 2000. Como veréis más adelante, la integración con este servidor es muy importante, por lo que muchos se preguntarán por qué no es posible combinar ambos en un mismo equipo. La incompatibilidad aparente entre estos viene dada por la utilización del mismo sistema de almacenamiento, para el cual ambos proporcionan todos los elementos necesarios y no pueden coexistir en la misma máquina.

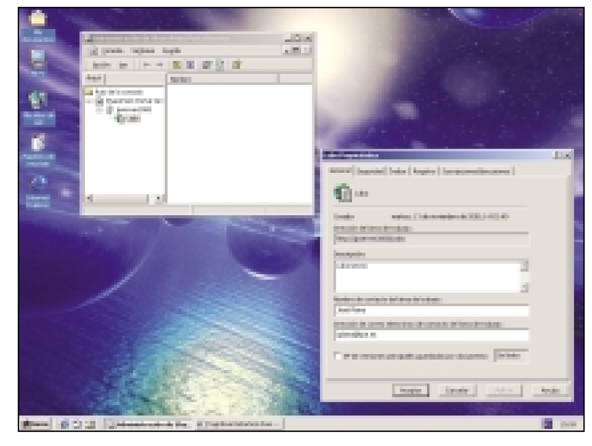


Por otra parte, los clientes necesitan también una pequeña instalación, que la podemos efectuar de forma automatizada utilizando un *script* en el *login* que cada usuario efectúa en el dominio. Básicamente, se trata de «accesorios» para Office y algunos elementos de infraestructura básica, como pueden ser las librerías MDAC (acceso a bases de datos) o el acceso a carpetas web.

En los dos casos, instalación del servidor y cliente es sencilla y rápida sin necesidad de introducir parámetro alguno. Tan sólo tendremos que concluir la instalación del cliente con un paso adicional: desde el icono *Mis Sitios de Red* hemos de crear un acceso directo al directorio donde se encuentra la web del portal. Si planeamos efectuar esta instalación en modo desatendido, muy probablemente tengamos que recurrir a algún *script* que efectúe esta tarea interactuando con el escritorio del cliente de forma automática.

Paso 2

Especificar los parámetros



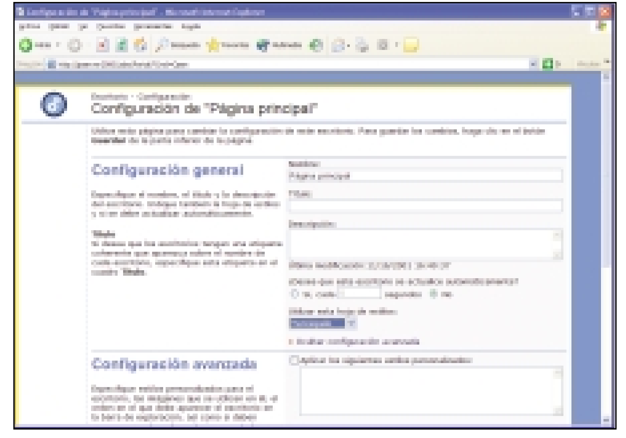
La configuración inicial del servidor la realizamos desde un MMC, accesible desde *Herramientas Administrativas* con el nombre de *Administración de SharePoint Portal Server*. Los parámetros básicos ya los hemos introducido durante la instalación, por lo que el acceso a esta aplicación se limitará a añadir usuarios y modificar algunos parámetros muy concretos. Dado que podemos crear múltiples portales (con la debida precaución ya que no se trata de sitios web convencionales y puede acabar saturando el servidor), pulsaremos sobre el que hayamos creado durante la instalación. A continuación, bajo la pestaña *Seguridad* incluimos los usuarios y sus funciones (lo más parecido a permisos que encontraremos dentro del programa) en el entorno. Estas pueden ser «Lector», «Autor» y «Coordinador», dependiendo siempre de los usuarios ya existentes en el dominio. Es por lo tanto el controlador de dominio el que proporciona la autenticación básica para estos servicios.



Paso 3

Personalizar el entorno

A partir de ese momento, el resto de configuración y preparación se efectuarán casi siempre desde un cliente. La parte más sencilla, y por el otro lado más cómoda para el administrador, será utilizar la misma página web del portal. En ella contamos en la parte superior con tres enlaces para la modificación del

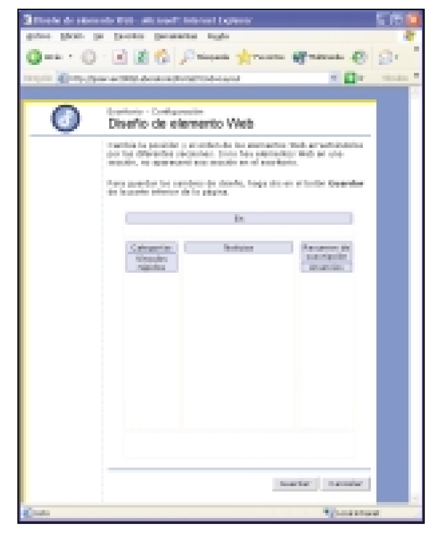


nuevo entorno de trabajo creado. Estos aparecen como *Contenido*, *Diseño* y *Configuración*. El último nos permitirá modificar parámetros como el título de la página, la descripción de esta o la simple combinación de colores para que se ajuste al diseño de la marca a la que representamos. Desplegando las *Opciones Avanzadas*, personalizaremos el logotipo que aparece en la parte superior izquierda, para lo que tan sólo tendremos que especificar una ruta a un archivo gráfico escogido y que se encuentra en el servidor. Si la página va a contar con contenidos muy dinámicos, también podremos modificar la frecuencia con la que se obligará al *Explorador* a refrescarse de forma automática.

Paso 4

Múltiples capacidades

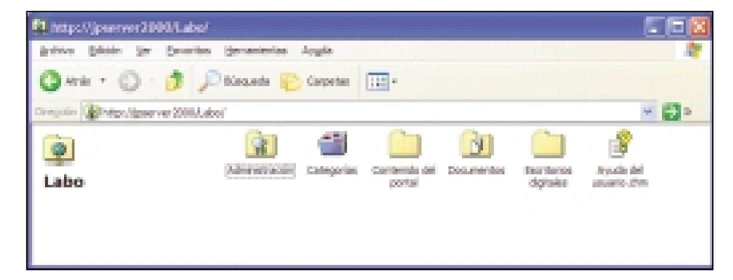
Lo visto hasta ahora es una mínima expresión de lo que puede llegar a ser este punto de entrada común para todos los usuarios de un departamento o empresa al completo. Pulsando sobre el enlace *Diseño*, una nueva página desvelará las verdaderas capacidades de personalización que dispone SharePoint. En esta se encuentran representadas en forma de módulos o cuadros cada una de las partes que componen la página, desde el encabezado hasta los enlaces. Pinchando y soltando estos módulos en otra parte de la página, desplazaremos estos rectángulos a un nuevo emplazamiento. Si retornamos a la página desde la que vinimos, veremos un cambio en su estructura completamente radical: seremos incluso capaces de cambiar el titular, de la parte superior a la parte más baja de la página.

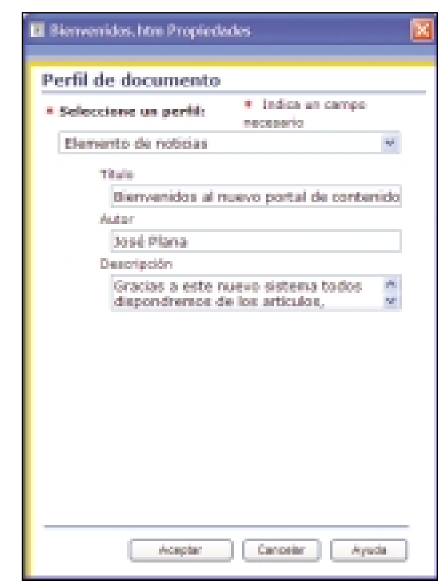


Paso 5

La clave de la aplicación

La funcionalidad más importante de la aplicación es la incorporación de nuevos documentos, archivos generados por Office, o simples páginas web con anuncios o textos simples. Para esto tendremos que abandonar el *Explorador* de forma temporal y dirigirnos a la carpeta web que creamos en *Mis sitios de red*.

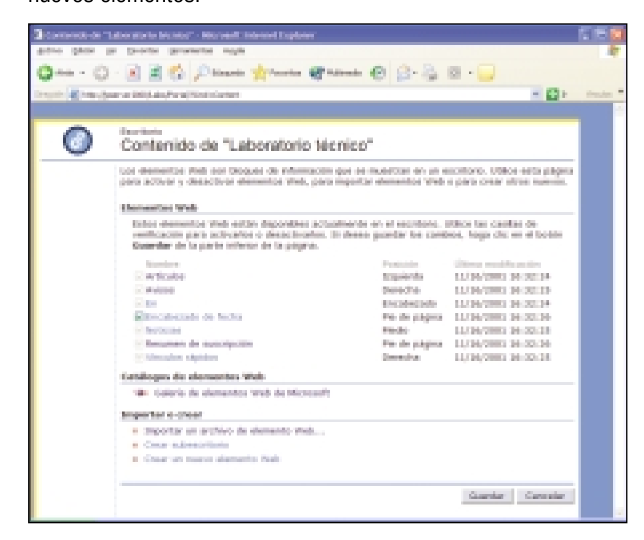




Dado el peculiar sistema de configuración que utiliza el programa, ésta dista mucho de una carpeta convencional. En ella se encuentras diferentes iconos, como si se tratase de programas, que determinarán la configuración del portal. Para la tarea de añadir contenidos, hemos de abrir la carpeta *Contenidos del Portal*. Dentro encontraremos otras tres nuevas clasificaciones, cada una con una función determinada: *Anuncios*, *Noticias*, *Resources* y *Vínculos rápidos*. Estas secciones se corresponden en su mayoría con los diferentes módulos o secciones que encontramos en la página web del portal. De esta forma, para añadir un nuevo elemento a la sección de *Anuncios*, crearemos o arrastraremos desde nuestro *Escritorio* un nuevo documento, por ejemplo, una página web, dentro de este contenedor. Si nos decantamos por el formato web, conviene que hayamos definido con anterioridad algún tipo de hoja de estilo para hacer más coherente la interfaz. Para determinar el aspecto con el que aparecerá dentro de la página del portal, pulsaremos sobre el icono con el botón derecho del ratón y seleccionaremos *Editar Perfil*. La nueva ventana nos permite, utilizando los diferentes campos de que dispone, modificar varios parámetros, aunque estos variarán en función del tipo de documento que vayamos a incluir, sea una noticia, anuncio o vínculo. De esta forma, en el campo *Título* debe constar el título de una noticia en el módulo del portal. Pero dependiendo del tipo de documento, variará también el comportamiento de ese parámetro, aunque no es complejo probar y ver qué es lo que ocurre exactamente, con una excepción, los vínculos. Estos funcionan de forma diferente ya que, independientemente del tipo de documento o contenido que incluya, no se representarán nunca. De hecho, lo mejor que podemos hacer es copiar un simple documento en blanco. Lo único que aparecerá realmente en el portal será el título de la página y el URL que tendremos que introducir en las propiedades.

Paso 6
Añadimos contenidos

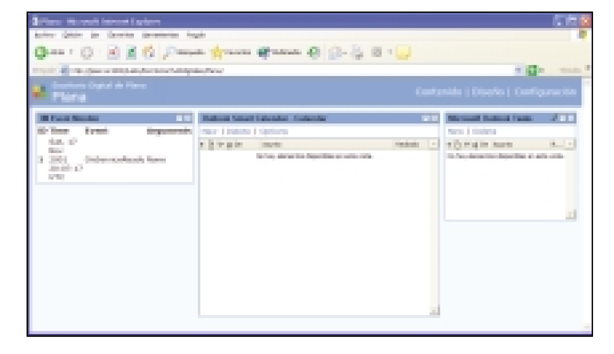
El siguiente paso debería ser algo más que añadir simples contenidos a nuestro portal. Recordaréis que en la página inicial del portal existía un vinculo junto a *Diseño* y *Configuración* etiquetado *Contenido*. Este nos conduce a la configuración de los módulos (por ejemplo Noticias, Avisos,...). Desde aquí podemos eliminar los módulos que se presentarán o añadir nuevos elementos.



En la página principal no podremos eliminar los ya disponibles, principalmente por motivos de funcionalidad. Sin embargo, nada nos impide añadir nuevos elementos. Microsoft denomina estos módulos descargables *Digital Dashboard* y existen varias formas de incorporarlos. Por un lado, en la web de Microsoft existe un pequeño catálogo en el que pulsaremos sobre una de las opciones y la incorporaremos. Otra forma de incluir elementos es descargarlos o crearlos nosotros mismos utilizando los kits de desarrollo de Microsoft, e importarlos desde un archivo. Encontraremos una buena biblioteca de estos accesorios en la página web de SharePoint (*www.microsoft.com/sharepoint/downloads/webparts*). Tan sólo tendremos que descargar alguno de los gratuitos (o de prueba) y comprobar su potencial.

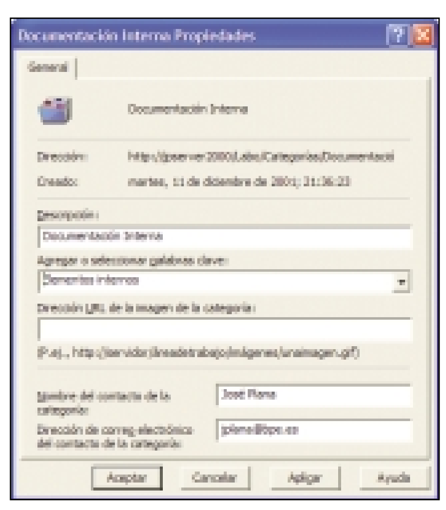
Paso 7
Creación de subsecciones

Siguiendo un buen ritmo de trabajo, en pocas horas habremos creado la estructura básica del portal, personalizando la mayoría de las opciones. Además es perfectamente factible, e incluso recomendable para algunos departamentos cuya tarea dista mucho de ser técnica, incluir las mismas herramientas de



trabajo dentro de la propia página. Estas subsecciones nuevas de la página se denominan *Escritorios digitales* y, en realidad, están enfocadas a sustituir las funciones del *Escritorio* que tienen los clientes en su PC. Para su creación, tan sólo tendremos que acudir al enlace *Administración* y, dentro de éste, *Crear un nuevo escritorio personal digital*. Un efecto parecido lo conseguiremos si dentro de la página a la que se accede a través del *link Contenido* seleccionamos *Crear un subescritorio*. Como muestra de la función que le podemos dar al *Escritorio* os mostramos por qué Exchange está tan relacionado con Sharepoint. Utilizando los *Webparts* descargados de la web de Microsoft, tenemos toda la funcionalidad de Outlook desde la página web del portal. Para ello, podemos escoger que sea este accesorio el encargado de mostrar las diferentes vistas o que sea el propio mecanismo de Exchange, mediante una página web.

Paso 8
Clasificación de documentos

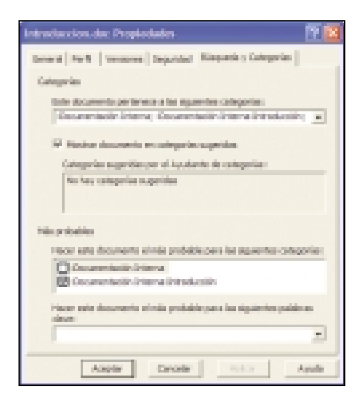


Pero si una clave de SharePoint es el intercambio y publicación de documentos, es muy importante que establezcamos algún mecanismo de clasificación para evitar que estos se pierdan. De no ser así, el mecanismo de distribución de documentos sería tan caótico como el que se utiliza habitualmente que implica carpetas compartidas. Para establecerlo, comenzaremos definiendo unos marcos que engloben la información a clasificar. De esta forma, si está bien definido, al hacer búsquedas de documentos, estos aparecerán mucho más rápidamente. Para ello nos dirigiremos a la carpeta web y crearemos todas aquellas clasificaciones bajo las que ordenaremos los documentos y contenidos externos, tal y como si se tratara de una carpeta. Además, a cada una de esta categorías le asignaremos una serie de palabras clave. Pulsando con el botón derecho del ratón, y escogiendo *Propiedades*, tendremos la oportunidad de añadir *Palabras clave* que acelerarán la búsqueda. Al englobar un documento dentro de una categoría, le estamos dotando de las mismas palabras clave que utiliza esa categoría, además de las propias que pueda contener el documento. Otras personalizaciones en estos menús pasan por el cambio del icono que lo representa en pantalla y la dirección de correo electrónico del representante.

Paso 9
Establecer las propiedades de los documentos

Para añadir documentos de trabajo, lo guardaremos bajo la carpeta web *Documentos*. Aunque también cabe la posibilidad de utilizar el propio portal para «subir» los documentos (utilizando el enlace *Biblioteca de documentos*), y de hecho se trata de un mecanismo perfectamente válido para aquellos clientes que únicamente dispongan de acceso mediante carpeta web, es preferible utilizar el siguiente método. Mediante

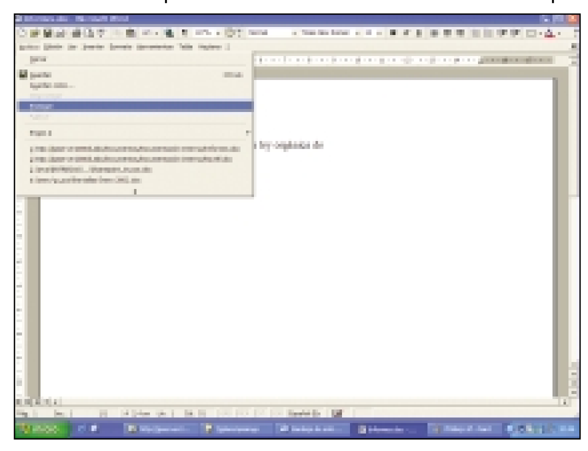
el botón derecho sobre el archivo y seleccionando la pestaña *Búsqueda y Clasificaciones,* podemos asignarle estas propiedades a los documentos de forma rápida, y siempre según las clasificaciones que hayamos creado con anterioridad. Por esto mismo, conviene definir un buen marco previamente para que sea el mejor descriptor de los contenidos de todos los archivos.



Paso 10

El proceso de publicación del documento

Ya comentamos la integración con Office pero, para hacerla efectiva, tendremos que encontrar primero las opciones. Normalmente el proceso que sigue un documento en producción suele estar determinado por el número de autores que trabajan durante su creación, revisores que lo aprueban y todo aquel que termina leyéndolo. Indudablemente, durante todas estas fases no es conveniente que más de una persona tenga acceso de escritura sobre el documento. Utilizando SharePoint los documentos no pueden ser editados de forma simultánea por

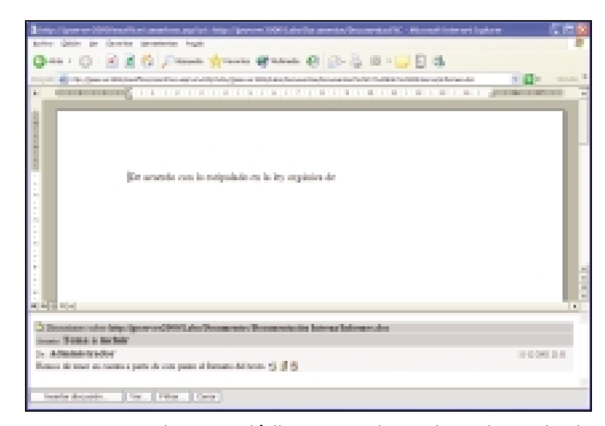


varios usuarios, evitando así incoherencias. Para esto Office añade algunas nuevas particularidades a su menú archivo. Al guardar un documento en la carpeta web del entorno de trabajo (bajo *Documentos*) veremos que algunas opciones nuevas se activan bajo el menú *Archivo*. Entre estas se encuentran *Proteger* y *Desproteger*. Mediante la primera evitamos que el documento se pueda modificar, sólo el autor podrá hacerlo. Cuando el documento no esté en este modo SharePoint se encargará de crear nuevas versiones de forma automática cada vez que lo actualicemos, quedando estas almacenadas en el servidor para su posterior consulta. La opción de *Publicar* supone que el documento se encuentra en su versión final y que, por lo tanto, puede ser accedido por cualquier visitante al foro.

Paso 11

Suscripciones y Discusiones

Dado que es muy posible que varias personas se encuentren trabajando en el mismo documento, las opciones de *Suscripciones* y *Discusiones* son de vital importancia. Aunque man-

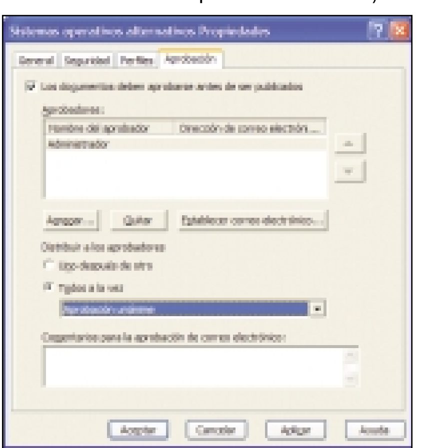


tengamos reuniones periódicas para determinar el estado de los documentos, no siempre será posible comentar en persona la sucesión de cambios y sugerencias. La primera nos notificará, mediante correo electrónico por ejemplo, cualquier modificación sobre un documento, o grupo de documentos si efectuamos la suscripción sobre una carpeta. Por otro lado, las *Discusiones* son sin duda más interesantes. Estas permiten comentar, utilizando algo similar a un foro de noticias, los contenidos del documento. De esta forma, los múltiples editores podrán comentar y poner en común opiniones con el autor o aquellos que finalmente aprueben el documento. Para acceder a estas opciones hemos de dirigirnos a la biblioteca de documentos y seleccionar el enlace adecuado sobre el documento con el que estemos trabajando. Gracias a la integración de Word (por decir alguna de las aplicaciones de Office) con Internet Explorer, veremos el primero dentro de la ventana de navegación a la vez que los comentarios de los participantes en la discusión. Por supuesto, el acceso a ambas herramientas se efectúa a través del portal, lo que simplifica enormemente el proceso.

Paso 12

Aprobación final del documento

Hasta ahora hemos hablado de «aprobar un documento» sin dar más detalles, sin embargo, es otra de las funciones que permite una colaboración más estructurada a la hora de elaborar un documento. De esta forma, definiremos con exactitud las funciones que pueden realizar cada uno de los usuarios sobre los documentos, y el proceso que debe seguir desde su creación hasta que está disponible.
Según la terminología de SharePoint, para pasar de un documento en edición a la fase de publicación (donde cualquiera puede acceder a él) es necesario que se «apruebe». Para configurar este proceso en alguna de las carpetas donde se encuentren los documentos, abriremos sus *Propiedades*; bajo la pestaña *Aprobación* se encuentran los parámetros principales. Bajo la lista de *Aprobadores* se encuentra el proceso necesario para que el documento se publique. Si optamos por *Uno después de otro*, todos lo miembros de la lista deberán dar su visto bueno (siguiendo además el orden especificado). Si escogemos *Todos a la vez*, bastará con que uno apruebe el documento o podemos obligar a que todos ellos (sin importar el orden) lo hagan.





datos a salvo

Instalar un servidor de *backup*

Intermedio

La continua aparición de nuevos virus, los fallos esporádicos que pueden tener nuestras máquinas o los posibles errores informáticos que se producen hacen tremendamente necesaria la realización de copias de seguridad periódicas. Lo ideal es contar con un servidor dedicado exclusivamente a estos menesteres, cosa que no todas las empresas pueden permitirse, ya que supone dejar una máquina inutilizada para realizar tareas de respaldo. En estos casos, una muy buena idea puede ser reutilizar ese viejo Pentium que muchos atesoran en el cuarto de los trastos porque sencillamente les da pena tirarlo. Ahora bien, estas máquinas, con un adecuado sistema de almacenamiento y, en caso de que fuera necesario, una ampliación de la memoria, son perfectamente capaces de cumplir con estas tareas.

Vamos a partir del supuesto de que tenemos un Pentium 200 MHz dotado de 32 Mbytes de RAM y un disco duro de 2 Gbytes en un estado inquietante. A partir de aquí, vamos a ver cómo convertir esta vieja máquina en nuestro nuevo servidor de *backups* en nuestra red informática.

Paso 1

La memoria de la máquina

Dependiendo de la configuración de la máquina, tendremos que decidir qué tipo de sistema operativo instalaremos. Para nuestro caso utilizaremos Windows 2000 Professional, el único que nos garantizará una correcta seguridad de los datos de todos los usuarios, tal y como más adelante veremos. Y aunque parezca imposible, un equipo Pentium a partir de los 133 MHz puede ejecutar Windows 2000 siempre que cuente con 64 Mbytes o más de memoria; por esta razón, ampliaremos la memoria de nuestra máquina hasta esa cifra como mínimo.

Paso 2

El eje fundamental del almacenamiento

Como punto clave de nuestro montaje encontramos el apartado de los discos duros. No podremos utilizar el disco que monta esta máquina para guardar nuestros preciados datos ya que, ni por capacidad, ni por fiabilidad será la opción más acertada. Habrá que buscar una solución mucho más inteligente. En nuestro caso nos vamos a decantar por utilizar una controladora RAID IDE de la compañía Adaptec, a la que conectaremos dos discos duros de 60 Gbytes cada uno. El fin de esta operación es doble: por una parte, la controladora soportará los últimos estándares de transmisión de los discos duros nuevos, por lo que obtendrá mejores prestaciones. Por otra, hará realidad el objetivo de la fiabilidad, ya que configuraremos la controladora en RAID Nivel 1. En este modo, se copiará exactamente la misma información en los dos discos duros con lo que, en caso de fallo de uno de ellos, el otro podrá recuperar la información sin que el usuario lo perciba.

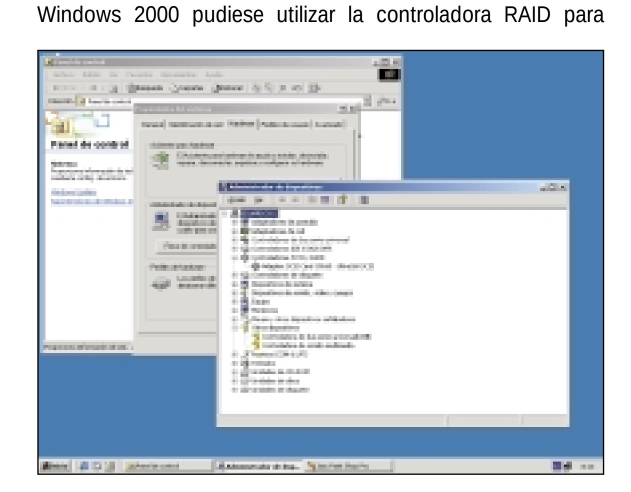
Y sobre el disco original de la máquina, lo mejor será eliminarlo directamente. Por ello, configuraremos la matriz de discos, crearemos dos particiones con «fdisk». A la primera partición le daremos 2 Gbytes, cantidad más que suficiente para realizar una instalación básica del sistema operativo. De esta manera, en los casi 58 Gbytes restantes crearemos otra partición que utilizaremos exclusivamente para guardar datos de los usuarios.

Paso 3

Configuración y puesta en marcha

Como en cualquier máquina que acabamos de levantar de cero, una vez instalado el sistema operativo (en nuestro caso Windows 2000 Professional) procederemos a instalar los controladores necesarios. El equipo que hemos utilizado como supuesto no ha necesitado que invirtamos una gran cantidad de tiempo en este aspecto ya que, tanto la tarjeta gráfica como el resto de elementos hardware, han sido reconocidos por el propio Windows 2000. Sólo fue necesario insertar los controladores de la nueva tarjeta de red que habíamos instalado.

Importante es también recordar que, para que la instalación de Windows 2000 pudiese utilizar la controladora RAID para

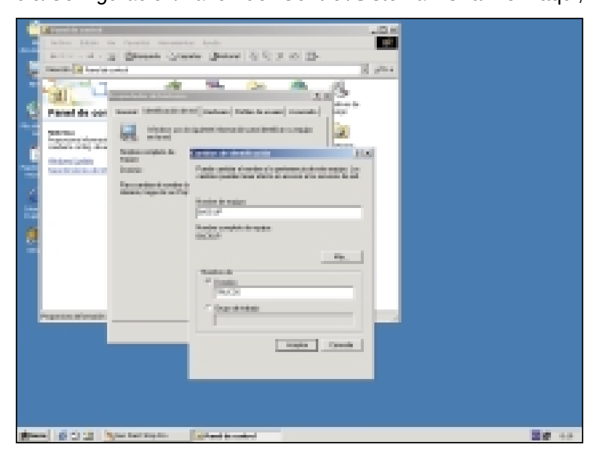


acceder a los discos, deberemos pulsar la tecla «F6» nada más comenzar la misma. Con ello, insertando el disco correcto, proporcionado por el fabricante de la tarjeta, podremos utilizar los discos manejados por la tarjeta para instalar el sistema operativo.

Paso 4

Agregar la máquina al dominio

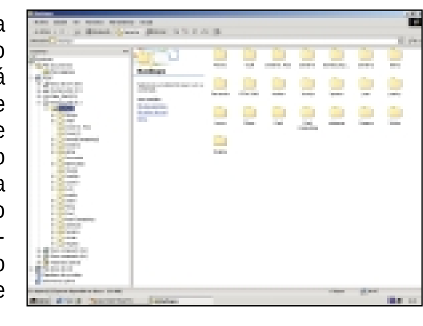
Para garantizar la absoluta seguridad en el acceso a los datos del servidor, nuestra máquina ha de ser agregada al dominio de la compañía. Para ello, en Windows 2000, acudiremos a *Inicio/Configuración/Panel de Control/Sistema*. Una vez aquí,



bajo la pestaña de *Identificación de red*, pincharemos en el botón *Propiedades*. En la nueva ventana que aparezca, en el apartado *Dominio*, no tendremos más que introducir el nombre del mismo. Se nos pedirá un nombre de usuario y contraseña con permisos para agregar equipos al dominio, como por ejemplo el administrador. Tras unos instantes, y si todo es correcto, aparecerá un mensaje dándonos la bienvenida al dominio.

Paso 5

Un directorio por persona

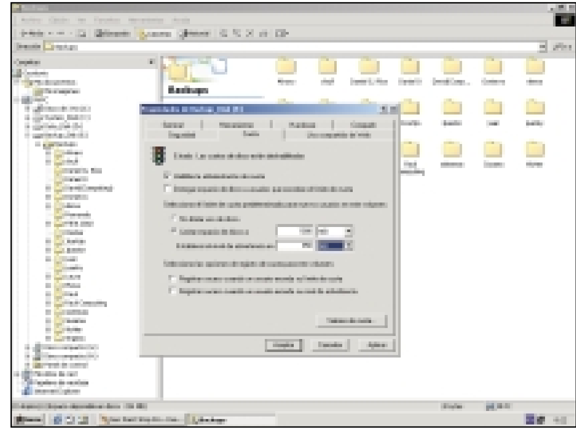


Tras reiniciar la máquina y acceder a ella con derechos de administrador, lo siguiente que habrá que hacer será crear un directorio por cada uno de los miembros o departamentos que deseamos que cuenten con su propio espacio virtual. De este modo, en la segunda partición iremos añadiendo tantos directorios como sea necesario, aunque será indiferente hacerlo desde *Mi PC* o desde el *Explorador* de Windows.

Paso 6

Habilitar cuota de disco

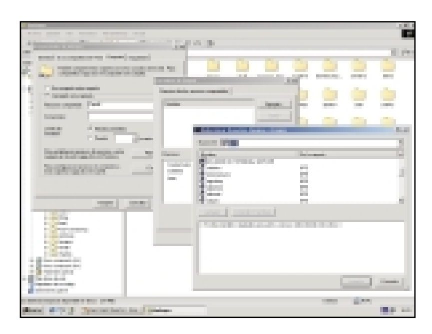
Será muy importante limitar la cantidad de espacio que cada usuario podrá utilizar en el servidor. Así, haremos clic con el botón derecho sobre el icono de la unidad en *Mi PC* o el *Explorador* de Windows, y seleccionaremos *Propiedades*. A continuación acudiremos a la pestaña *Cuota*, donde marcaremos la opción *Habilitar la administración de cuota*. Justo debajo veremos cómo se activan una serie de opciones, donde podremos



indicar el espacio exacto que se asignará por usuario, así como el momento en el que se le lanzará una advertencia. Haremos clic sobre *Aceptar* y a partir de ese momento, tendremos a todos los usuarios controlados.

Paso 7

Permisos y ocultar carpetas



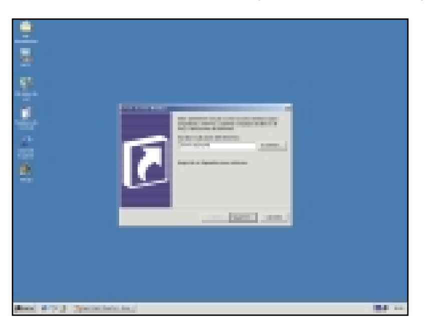
El siguiente paso será compartir y proteger una a una todas las carpetas. Esto se lleva a cabo haciendo clic con el botón derecho del ratón sobre cada una, seleccionando *Compartir* y marcando la opción *Compartir esta carpeta*. En el nombre del recurso compartido podremos poner el que prefiramos, aunque añadiéndole un signo «$» al final. De esta manera, el recurso estará oculto y no aparecerá listado en red. Esto evita, no que se acceda al directorio, pero sí que el resto de usuarios de la red sepa quién tiene o no su directorio de *backup* propio y puedan surgir deseos de acceder a su información.

Para el control de accesos pulsaremos sobre *Permisos*. En la siguiente ventana eliminaremos el usuario *Todos*, pulsaremos *Agregar* y seleccionaremos el único usuario del dominio que tendrá acceso a ese directorio. Por último, no podemos olvidar bloquear la máquina («Ctrl+Alt+Supr»/ *Bloquear equipo*) para que nadie pueda acceder a la información contenida en ella con sólo sentarse delante.

Paso 8

Acceder a las carpetas

El último paso será crear accesos directos desde cada una de las máquinas a la correspondiente carpeta del usuario en la red. En el mismo *Escritorio* bastará con hacer clic con el botón derecho, y seleccionar *Nuevo/Acceso directo*. En la nueva ventana escribiremos una ruta del estilo de *\\backup\pepe$*. Una vez creado este acceso, y siempre que el usuario del dominio autorizado para acceder a esa carpeta sea el mismo que ha iniciado sesión en la máquina, se podrá visualizar el contenido de ese espacio virtual.





Todo controlado

Inventario y documentación

Intermedio

Aunque no sea ni mucho menos imprescindible, y en cierta forma se salga un poco de la línea de temas prácticos que hemos tratado alrededor de una intranet informática, no podíamos dejar de hablar del inventariado y documentación de la infraestructura. Para ello, os adelantamos algunos consejos prácticos que seguramente os serán de utilidad para empezar a valorar esta clase de tareas que, a la larga, suelen resultar útiles, al tiempo que permiten ahorrar tiempo y dinero.

Paso 1

Las máquinas al detalle

Lo primero que habrá que hacer para documentar e inventariar correctamente toda nuestra maquinaria informática se centra en crear un entorno amigable para nosotros donde depositar y consultar esa información. Para ello, lo mejor es hacerse con una base de datos tipo Access, con la que podremos crear múltiples tablas dedicadas a ordenadores, impresoras, monitores, accesorios, etc. Lo más recomendable sería asignar a cada PC un número de serie que nos permitiese conocer, en todo momento, su configuración e incluso información detallada sobre sus contraseñas de acceso, número de serie de su sistema operativo, averías sufridas o usuarios que lo han utilizado. Es por ello que lo recomendable sería crear un gran tabla dedicada, por ejemplo, solamente a ordenadores. En ella, declararemos los campos de cada información que deseamos tener a mano: identificación, procesador, memoria, disco duro, dirección IP, sistema operativo, etc.

Cuando más detallada sea esta información, más nos costará elaborarla y mantenerla. Pero, al contrario de lo que se pueda pensar, más nos podrá ayudar en un momento dado. En todo momento podremos listar el número de máquinas y la configuración de cada una de ellas. En caso de desastres o robos, contratación de seguros o valoración de las propiedades de la compañía resultará muy útil.

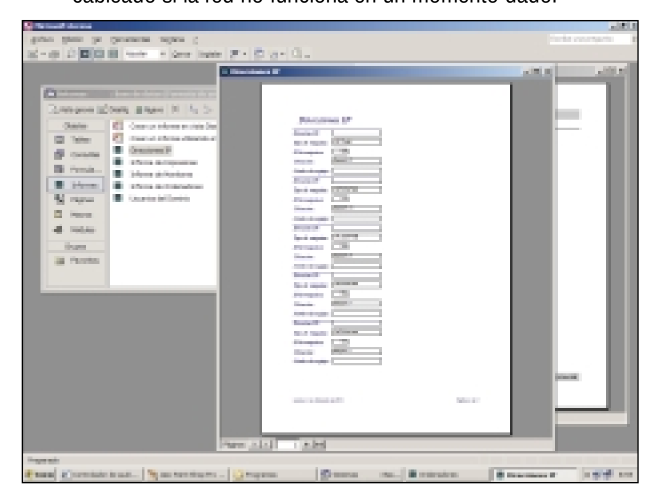
Algo parecido ocurre con los *routers*, *hubs*, impresoras, monitores y demás accesorios. En el caso de las impresoras, por ejemplo, podremos anotar junto a los lógicos «marca y modelo», la referencia del consumible. De esa manera, cuando un usuario nos pida un nuevo cartucho, no tendremos más que consultar la referencia y solicitarla a nuestro proveedor informático.

Paso 2

Documentación exhaustiva

Este es otro de los aspectos más relevantes que hemos de tener en cuenta a la hora de organizar nuestra estructura. Si montamos un sistema de antivirus en red, nada mejor que realizar un documento en el que se explique qué hemos instalado, cuál es la versión, su forma de funcionamiento, frecuencia de actualizaciones, teléfonos de atención al cliente e, incluso, nuestro número de cliente. En definitiva, toda clase de aplicaciones que trabajen en red y que tengan cierta complejidad técnica son susceptibles de ser reflejadas en uno de estos documentos. Puede que dentro de unos meses e incluso años, no recordemos cómo trabajaba una determinada aplicación, ni qué servidores utilizaba para funcionar.

Por supuesto, la red tendrá que ser otro de los grandes apartados. Guardar correctamente la configuración de nuestro *router* (su IP, direcciones DNS y los servidores de correo) será clave para resolver rápidamente futuros problemas. De la misma forma, en la base de datos del inventario informático, podemos crear una tabla específica con las direcciones IP utilizadas y libres, nombre de usuario y contraseñas del dominio e, incluso las correspondencias físicas entre los puertos del *hub* o *switch* y cada uno de los puestos de trabajo. Y es que esta última información podría sernos útil para verificar el cableado si la red no funciona en un momento dado.





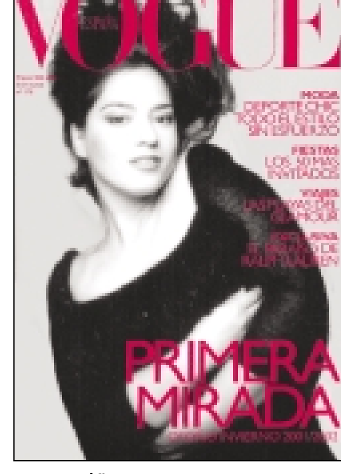
Optimizar imágenes para la Web

Todos los formatos utilizados y las claves para acelerar la visualización

Intermedio

Cada día son más las personas que tienen su propia página web y se preocupan por su apariencia, diseño y rapidez de carga. El inconveniente más habitual al tener acceso a estas páginas es la larga espera que supone el proceso de descarga y visualización de los gráficos. Es muy importante tener en cuenta este detalle, ya que los internautas no esperan más de un minuto en la carga de una página.

La optimización es el proceso de ajustar con precisión la calidad de visualización y el tamaño de archivo de una imagen para su uso en la Web u otro medio en línea. Muchos programas de retoque fotográfico ofrecen un rango efectivo de controles para comprimir el tamaño de archivo de una imagen, a la vez que optimizan la calidad de visualización en línea. Podemos optimizar las imágenes en los tres principales formatos de archivos gráficos utilizados en la Web: GIF (Formato de Intercambio de Gráficos), JPEG (*Joint Photographic Experts Group*) y PNG-8 o PNG-24 (Gráficos de red portátiles, con color de 8 o 24 bits).



¿Cómo podemos hacer que nuestra página con gráficos sea rápidamente visible? La respuesta está en la optimización de esos gráficos e imágenes, en utilizar todos los recursos posibles para que, sin perder apenas calidad, la rapidez de descarga sea mayor. En la utilización de las herramientas de optimización de imágenes para Internet se unen las expectativas de los *webmasters* (páginas con poco peso) y los diseñadores (presentaciones atractivas para el usuario). Por otra parte, debemos tener siempre presente que hay muchas personas que tienen desactivada la opción de descarga de imágenes de su navegador, por lo que tenemos que intentar que nuestra página sea igualmente legible con o sin gráficos.

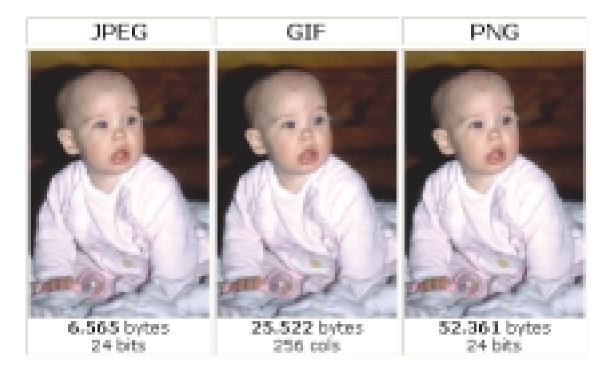
Formatos de imágenes usados en Internet

Los formatos más utilizados, debido a que son soportados por todos los navegadores y por su capacidad de compresión, son JPEG y GIF. También existe una alternativa más moderna: el formato PNG, en sus dos versiones, el PNG-8 y el PNG-24.

Paso 1

Formato JPEG o JPG

Fue elaborado por *Joint Photographic Experts Group*, de ahí su nombre. Es un formato que se puede utilizar libremente sin tener que pagar derechos por ello. Al comprimir las imágenes en JPEG, se produce una pérdida de calidad pero ésta es imperceptible al ojo humano, con lo cual la imagen puede ser aparentemente igual a la original si elegimos un nivel de compresión pequeño, ya que otra ventaja de JPEG es que permite elegir el nivel de compresión que queremos para nuestro archivo. Técnicamente JPEG realiza un promedio de color de los *pixels* por zonas, por lo cual este formato es ideal para las

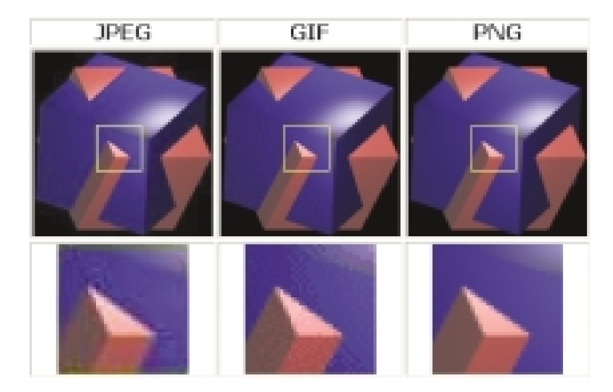


imágenes en las que se presentan tramas, degradados o matices de color y lo hace menos útil en aquellos gráficos de colores planos o de trazos muy definidos. JPEG ofrece la posibilidad de guardar los archivos en modo progresivo. Esta modalidad permite que aunque la imagen no se haya cargado completamente, aparezca con poca calidad y según se vaya cargando la página ésta vaya aumentando hasta llegar a la calidad final.

Paso 2

Formato GIF

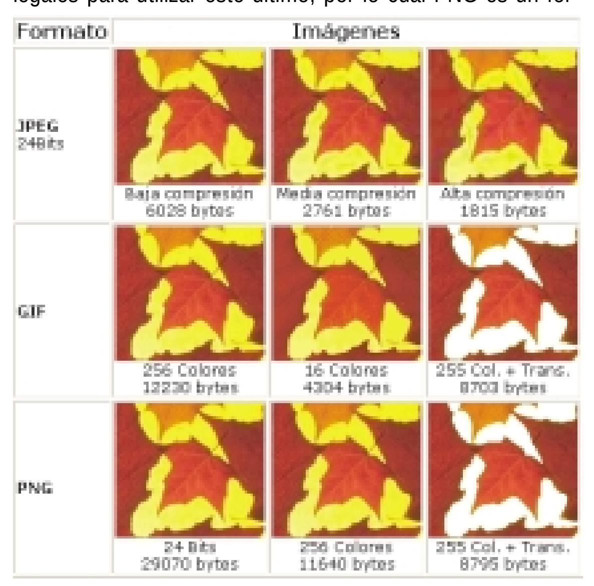
Sus siglas provienen de *Graphic Interchange Format*. GIF es un formato que utiliza el algoritmo LZW (el mismo que utiliza ZIP), del cual es propietario Unisys y por el que repentinamente en 1995 se decidió que cualquier software que ofreciera la



posibilidad de mostrar o crear GIF tendría que pagar derechos a Unisys y CompuServe (creadora del formato GIF). Incluso es posible que se llegue al extremo de cobrar derechos a cualquiera que utilice este formato, lo cual ha generado que se inicien campañas en contra de su utilización.
Es un formato de compresión sin pérdida y tiene una profundidad de color de 8 bits, lo que le permite tener un máximo de 256 colores. Por eso, este formato está especialmente indicado para dibujos lineales o imágenes con pocos colores y apenas degradados. Los colores de los archivos GIF aparecen representados en una tabla y se pueden elegir y cambiar por otros. Además, estos archivos se pueden grabar con formato «entrelazado», lo que hace que vaya apareciendo (al cargarse en una página web) la imagen progresivamente, de forma similar al modo «progresivo» de JPEG. Una de las grandes ventajas de GIF es que permite crear animaciones uniendo varias imágenes a modo de fotogramas: es lo que se conoce como GIF animado. También ofrece la posibilidad de que uno de los colores de la imagen se establezca como color transparente, lo cual puede ser muy útil si nos interesa que aparezca algo que hay debajo de nuestra imagen o para hacer las esquinas redondeadas (muy utilizado para hacer botones).

Paso 3
Formato PNG

PNG es un acrónimo de *Portable Network Format* y nació como alternativa al formato GIF debido a los problemas legales para utilizar este último, por lo cual PNG es un formato completamente libre que cualquiera puede utilizar sin tener que pagar derechos por ello. Se trata de un formato muy prometedor. Para empezar, soporta una profundidad máxima de color de 24 bits, es decir, 16,7 millones de colores que, frente a los 256 de GIF, lo hacen francamente atractivo. Su sistema de compresión se denomina LZ77 y, al igual que el LZW, comprime sin perder información. Los archivos PNG pueden guardarse en modo «entrelazado» y posee la cualidad de tener un «canal alfa», lo que significa que es un formato que no sólo permite transparencias sino que esa transparencia puede tener diferentes grados. Aún no permite realizar animaciones pero se está trabajando en crear una versión de PNG que sí lo haga posible y que se llamará MNG. El inconveniente principal de este formato es que, al ser tan nuevo, las versiones más antiguas de los navegadores no lo soportan y eso hace que no esté muy generalizado. Hay dos tipos: el PNG-8 y el PNG-24. El primero usa 8 bits de color y el segundo 24. Este último también soporta transparencia multinivel que nos permite preservar hasta 256 niveles para suavizar los bordes de una imagen con cualquier color de fondo. Sin embargo, esta característica no es soportada por todos los navegadores.



Paso 4
Qué formato elegir

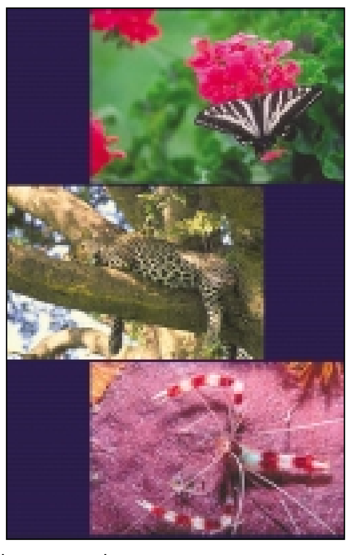
Ahora que ya conocemos los formatos óptimos para incluir imágenes en nuestra página web, hemos de decidir, según las características de nuestras fotos, iconos o material gráfico, qué formato utilizar. Por supuesto, podemos utilizar varios formatos en la misma página web: no todos nuestros gráficos tienen que ser necesariamente GIF, JPEG o PNG, podemos alternarlos o no dependiendo de cómo sean nuestras imágenes.



Habitualmente hay un formato que prevalece sobre los demás según el tipo de imagen que tengamos. Así, para los iconos es más utilizado el formato GIF ya que, al ser pequeños y con pocos colores, se obtiene una calidad óptima a un tamaño de archivo realmente pequeño. Para las *fotografías* el más utilizado es el formato JPEG ya que suele tener muchos más colores, matices y degradados (fondos de cielo, mar, campo), por lo que nos ofrecerá una buena definición de la fotografía y el mejor tamaño posible para esa definición. Como vemos, la regla general se resume en que cuando hay pocos colores, lo ideal es utilizar el formato GIF y, si hay muchos, el mejor formato es el JPEG. Lo ideal sin embargo es comparar tamaños y calidad usando varios formatos para una misma imagen y al final decidir el que nos parezca mejor, puesto que no siempre se obtiene el resultado esperado aplicando el formato que, en principio, parecía el adecuado.
Para guardar nuestra imagen con uno de los formatos mencionados anteriormente necesitamos un programa de tratamiento de imágenes, ya sea Photoshop, Paintshop Pro, CorelDraw, etc. Nosotros vamos a centrarnos en el programa más utilizado para tratar imágenes: Adobe Photoshop.

Paso 5

Cómo acelerar la visualización



La primera opción que hay que tener en cuenta es que los gráficos tardan en cargarse o que el internauta puede tener la opción de carga automática de gráficos desactivada. Si usamos gráficos decorativos de manera indiscriminada, una página web puede parecer extraña y confusa si no se visualizan dichos gráficos. El tiempo que tarda la página en cargarse completamente es de gran importancia. Un usuario no va a esperar más de unos segundos a que una página termine de cargarse. Por esto, una buena norma es que el tamaño total de todas nuestras imágenes no supere los 50 Kbytes, que un módem de 28 Kbps tardará unos 15 segundos en cargar. Otra buena idea es usar siempre los atributos *HEIGHT* y *WIDTH* al insertar una imagen en la página web. Esto hace que el navegador sepa el tamaño de la imagen antes de que empiece a cargarla, lo que permite reservar espacio en la página. De esta forma, la página se dibuja con los espacios vacíos que serán rellenados con las imágenes cuando éstas se carguen. Con esto se consigue que la página se visualice completa antes, sin tener que esperar a la carga de las imágenes. Algo también a tener en cuenta sería aprovechar la «Carga progresiva» de la que disponen los formatos gráficos. Esto permite que se pueda visualizar una imagen incompleta del gráfico mientras éste todavía se está cargando. Esta característica en los formatos GIF y PNG se llama «entrelazado» y en el formato JPEG, «progresivo». Por último, otro pequeño truco es usar la misma imagen tantas veces como nos sea posible. De esta manera aprovechamos la característica con que cuenta la mayoría de los navegadores de almacenar en la caché imágenes ya cargadas. Con esto aceleraremos notablemente la carga de las páginas.

Photoshop e ImageReady

Photoshop incluye desde su versión 5.5 una aplicación para preparar y editar gráficos para la Web llamada ImageReady. Con esta aplicación es muy sencillo transformar nuestras imágenes en formatos óptimos para ser visualizadas en Internet. Actualmente, la última versión del popular programa de retoque fotográfico es la 6.0, que viene acompañada con el ImageReady 3.0



Formas de guardar las imágenes optimizadas

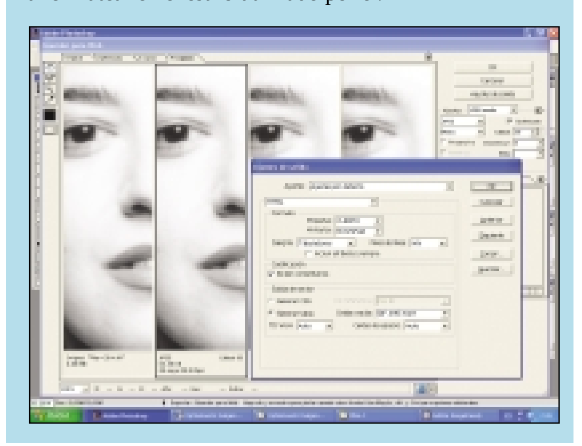
Hay varios modos de hacer esto para la Web.

HTML e imágenes: Es posible generar todos los archivos necesarios para utilizar la imagen como una página web. Esto incluye un archivo HTML y archivos de imágenes independientes para los sectores de la imagen origen. El archivo HTML incluye código para todos los efectos Web, como enlaces de hipertexto, mapas de imágenes, *rollovers* y animaciones en el documento. Los archivos de imagen utilizan el formato y las opciones especificadas en el ajuste de optimización.

Sólo imágenes: Es posible guardar la imagen sólo con el formato y las opciones especificadas en el ajuste de optimización. Si la imagen de origen contiene varios sectores, cada uno se guarda como un archivo independiente.

Sólo HTML: Permite guardar el código HTML para la imagen, pero no los datos de ésta. En ImageReady, también podemos crear un archivo HTML mediante el comando *Copiar HTML*. Este comando permite copiar el código HTML para una imagen optimizada en el portapapeles y pegar el contenido HTML en un archivo del mismo tipo. Si posteriormente realizamos cambios en la imagen origen, usaremos el comando *Actualizar HTML*.

Con ImageReady podemos seleccionar la opción de *Incluir código GoLive* para volver a formatear el código HTML y JavaScript para que los *rollovers* puedan editarse completamente en Adobe GoLive. El código se vuelve a formatear en el estilo utilizado por él.



Paso 6

Métodos de optimización de imágenes

Para una optimización básica, el comando *Guardar como* permite guardar una imagen como un archivo GIF, JPEG o PNG. Según el formato de archivo, podemos especificar la calidad de imagen, transparencia o halos de fondo, visualización del color y método de descarga. Sin embargo, no se preserva ninguna característica Web que hayamos añadido al fichero, como sectores, enlaces, animaciones o *rollovers*.

Para una optimización precisa podemos utilizar las funciones de optimización de Photoshop o ImageReady para previsualizar las imágenes optimizadas en diferentes formatos de archivo y con diferentes atributos. Contamos con la posibilidad de



ver varias versiones de imágenes a la vez y modificar los ajustes de optimización conforme previsualizamos la imagen para poder seleccionar la combinación de ajustes que mejor se adapte a nuestras necesidades. También tendremos la alternativa de especificar la transparencia o halos de fondo, seleccionar opciones para controlar el tramado y redimensionar la imagen hasta unas dimensiones o porcentaje de tamaño determinadas. Cuando guardamos una imagen optimizada mediante el comando *Guardar para Web* (Photoshop) o *Guardar optimizada* (ImageReady), podemos seleccionar la opción de generar un archivo HTML para la imagen. Este archivo contiene todo el código necesario para visualizar la imagen en un navegador Web, así como los enlaces, *rollovers* y animaciones. Para ver las imágenes durante la optimización, en Photoshop deberemos seleccionar *Archivo / Guardar para Web*. En ImageReady, podemos ver y trabajar con imágenes optimizadas en cualquier momento en la ventana de documento.

Paso 7

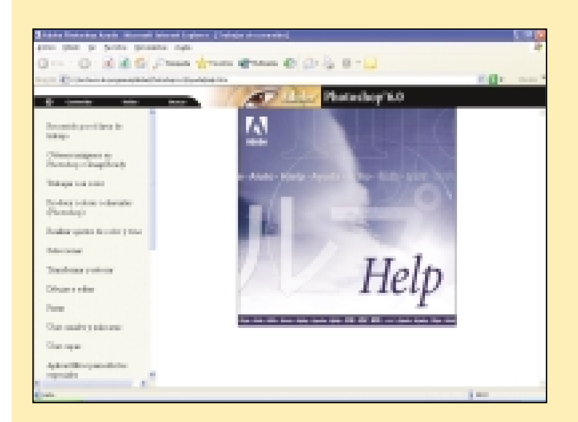
Visualización de las imágenes

Las opciones de presentación en Photoshop e ImageReady permiten cambiar con facilidad entre la versión optimizada y la versión original (no optimizada) de una imagen y ver a la vez hasta cuatro versiones de una imagen optimizada. Para seleccionar una opción de presentación de las fotos, hay que hacer clic en la parte superior de la imagen y elegir entre *Original* si queremos ver la imagen sin optimizar, *Optimizado* para ver la imagen con los ajustes de optimización actuales aplicados, *2 copias* cuando queramos ver dos versiones de la imagen, una al lado de la otra, y *4 copias* para ver cuatro versiones de la imagen.



Si seleccionamos la vista de *2 copias* o *4 copias*, Photoshop o ImageReady determinan una composición para la imagen según la proporción (anchura / altura) de la imagen. Las fotos pueden aparecer en una composición vertical, horizontal o de 2 x 2 (dos filas y dos columnas). Esta última composición sólo está disponible para la vista de 4 copias. Tendremos la posibilidad de seleccionar una versión de la imagen en la vista de 2 o 4 copias para aplicarle nuevos ajustes de optimización. También podremos automáticamente *repoblar* las vistas, es decir, generar nuevas versiones optimizadas de la imagen según la versión seleccionada. También es posible hacer que una versión optimizada vuelva a la versión original de la imagen. En ImageReady podemos cambiar los ajustes de optimización por defecto en *Preferencias de optimización*. Ambos programas generan menores versiones optimizadas de la imagen según los ajustes de optimización de la versión seleccionada. Ambas versiones, la seleccionada y la original, no se ven alteradas durante la repoblación si están presentes. Por esta razón, la opción *Repoblar vistas* funciona con la vista de *2 copias* sólo si la versión original de la imagen no está presente.
Mientras vemos la imagen durante la optimización, si no es posible una visualización completa de la misma, podemos «navegar» por las diferentes áreas. Esto es particularmente práctico con las vistas de 2 y 4 copias. En ImageReady además podemos usar el comando de *Ajustar en pantalla* para ver la imagen entera en el espacio disponible. Si vamos a navegar debemos seleccionar la herramienta *mano* en el cuadro de diálogo *Guardar para Web* (Photoshop) o en *Caja de herramientas* (ImageReady).

Imágenes de fondo

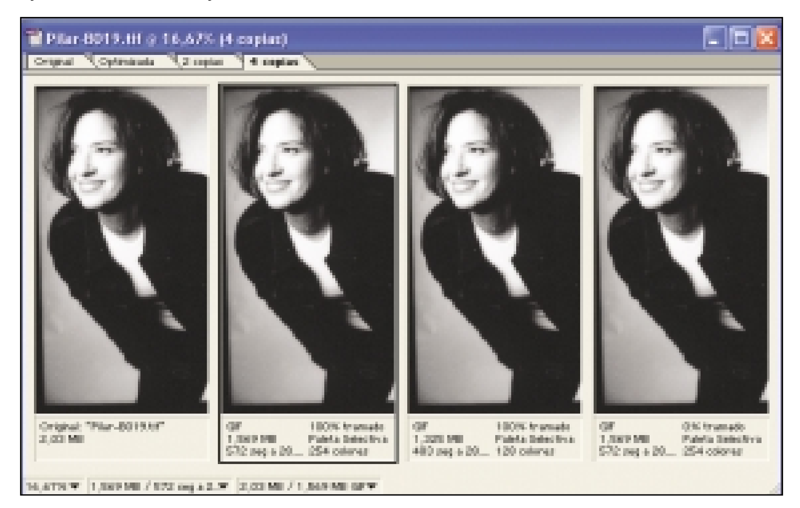


Muchas páginas web contienen imágenes de fondo en formato de mosaico, creadas a partir de un solo gráfico repetido cuantas veces fuera necesario para rellenar toda la página. En ImageReady, podemos crear un archivo HTML que mostrará la imagen actual como un fondo en mosaico en un navegador Web. También podemos crear un archivo HTML que mostrará otra imagen o un color uniforme como fondo detrás de la imagen actual. ImageReady incluye la etiqueta *<body background>* para el color de fondo en el archivo HTML. Además, podemos preparar una imagen para utilizarla como fondo en mosaico utilizando el filtro *Creador de azulejos*, que fusiona los bordes de una imagen para crear un fondo sin grietas. También puede utilizar el filtro *Creador de azulejos* para crear un fondo de caleidoscopio, en el que una imagen se voltea horizontal y verticalmente hasta crear un diseño abstracto.

Paso 8

Optimización de imágenes

Para optimizar una imagen para la Web, seleccionamos un formato de archivo y otras opciones en el panel *Optimizar* (Photoshop) o en la paleta *Optimizar* (ImageReady). Podemos aplicar distintos ajustes de optimización a diferentes sectores de una imagen. También es posible usar canales alfa para optimizar de forma selectiva dentro de un sector o entre sectores. Photoshop e ImageReady incluyen varios ajustes con nombres predefinidos. Cuando definimos ajustes de optimización de manera que no coinciden con un conjunto que disponga de nombre, el menú *Ajustes* muestra la expresión *Sin nombre*.
Por otro lado, también es posible optimizar una imagen o sector en un tamaño de archivo aproximado. Esta función permite alcanzar rápidamente un tamaño del fichero deseado sin tener que probar diferentes ajustes de optimización. Para ello debemos seleccionar *Optimizar a tamaño de archivo*. Allí encontraremos dos opciones: una que nos permite dejar los ajustes actuales y otra denominada *Autoseleccionar*

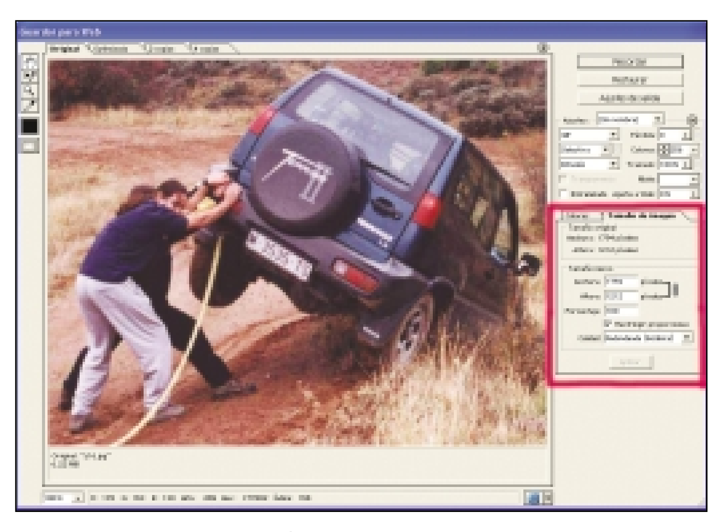


GIF/JPEG, que genera automáticamente un GIF o un JPEG. Por último, deberemos seleccionar: *Sector actual* para optimizar el sector seleccionado en aproximadamente el tamaño de archivo especificado; *Todos los sectores por separado* para optimizar cada sector de una imagen en el tamaño de archivo especificado, aproximadamente, y *Todos los sectores juntos* si queremos optimizar la suma del tamaño de todos los sectores con el tamaño del archivo especificado. El valor total se reparte entre los sectores individuales según el tamaño relativo de cada uno de ellos.

Paso 9

Redimensionar la imagen en Photoshop

En Photoshop, cuando se optimiza una imagen, se puede redimensionar hasta un número específico de *pixels* o hasta un porcentaje del tamaño original. Tan sólo tenemos que hacer clic en *Tamaño de imagen* del cuadro de diálogo *Guardar para Web*. Podemos incluso restringir las proporciones para mantener la anchura y la altura, aunque un parámetro muy significativo es el de *Interpolación* del menú *Calidad*. Hay dos tipos. Irregular (por aproximación) es el método más rápido aunque menos preciso. Se recomienza utilizarlo en las ilustraciones que contienen bordes no suavizados para preservar bordes irregulares y producir archivos menores. El otro método es *Redondeada* (bicúbica), que es el más

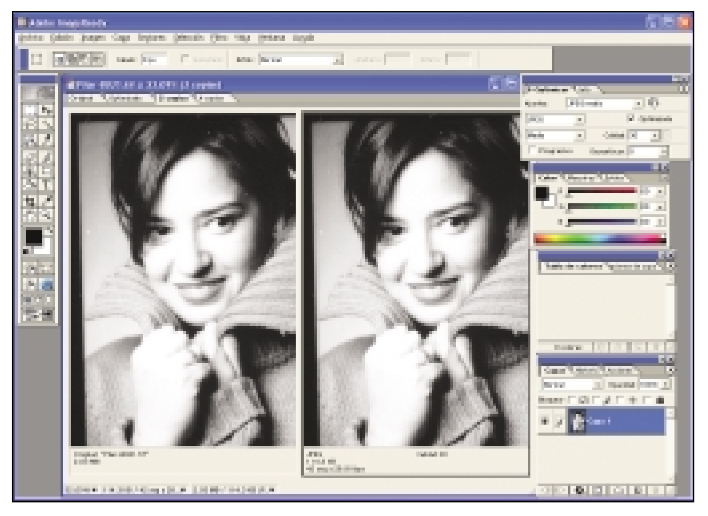


lento pero el más preciso, lo que da como resultado tonalidades más suaves.
Por defecto, Photoshop e ImageReady regeneran automáticamente la imagen optimizada cuando se hace clic en *Optimizado*, *2 copias* o *4 copias* de la parte superior del documento (si se ha modificado la imagen desde la última optimización), cuando se cambian los ajustes de optimización con la imagen visualizada o cuando se edita la imagen original.

Paso 10

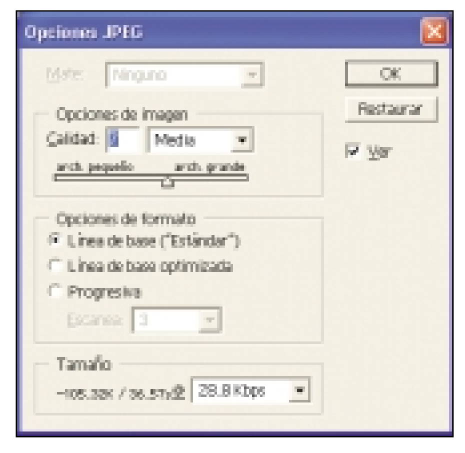
Controlar la optimización en ImageReady

En ImageReady podemos desactivar la *Auto-regeneración* de manera que la última versión de la imagen optimizada permanezca en la ventana de la imagen hasta que, manualmente, se optimice de nuevo la misma o se reactive la *Auto-regeneración*. Esta función es útil si deseamos editar la imagen sin tener que detenernos para la reoptimización con cada modificación. También puede cancelar la optimización mientras está en progreso y preservar la imagen previa. Cuando se desactiva la *Auto-regeneración*, el botón *Regenerar* aparece en la esquina inferior derecha de la vista de cada imagen optimizada. Un símbolo de aviso de regeneración también aparece en la paleta *Tabla de colores* si la imagen optimizada está en formato GIF o PNG-8, lo que indica que la tabla de colores ha caducado.



Paso 11

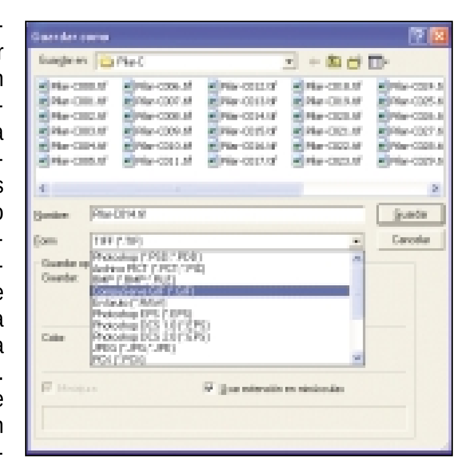
Definir opciones de optimización para el formato JPEG



Cuanto más alta ajustemos la calidad, más detalle preservará el algoritmo de compresión. Sin embargo, el uso de un ajuste de calidad alto produce un archivo de mayor tamaño que el uso de un ajuste de calidad bajo. Lo ideal es ver la imagen optimizada con varios ajustes para determinar el mejor equilibrio entre calidad y tamaño del archivo. Para crear un JPEG mejorado con un tamaño de archivo ligeramente menor, seleccionamos *Optimizado*. Este se recomienda para una máxima compresión de archivo, sin embargo, algunos navegadores antiguos no admiten esta función. Otra opción es *Progresivo* para crear una imagen que se visualice progresivamente en un navegador Web. La imagen se visualizará como una serie de superposiciones, permitiendo a los usuarios ver una versión de baja calidad antes de descargarla totalmente. Este método requiere el uso del formato JPEG Optimizado y más memoria RAM para su visualización y algunos navegadores no lo admiten. Si desenfocamos la imagen para redondear bordes mal acabados, debemos introducir un valor en el campo *Desenfocar*. Esta opción es idéntica a un filtro de *Desenfoque gaussiano* y permite una mayor compresión del archivo, con lo que se disminuye el tamaño del archivo. Lo ideal es un ajuste entre el 0.1 y 0.5. Por último, si la imagen original contiene transparencias, debemos seleccionar un color mate que coincida con el fondo de la página Web.

12

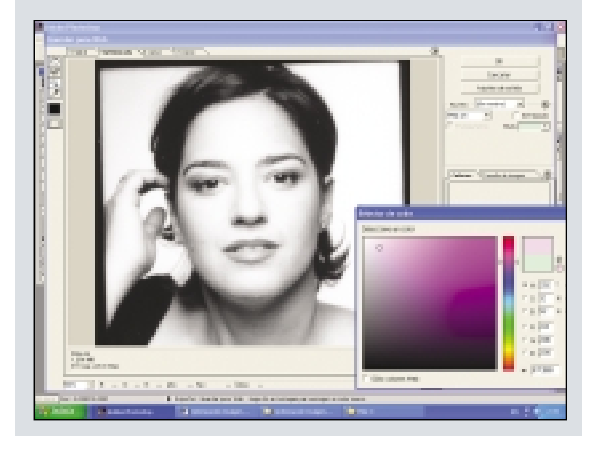
Definir opciones de optimización para el formato GIF y PNG-8



Para el formato GIF, podemos arrastrar el regulador de pérdida o introducir un valor que permita la compresión por pérdida. Ésta reduce el tamaño del archivo, ya que descarta datos de forma selectiva; cuanto mayor sea el «ajuste de pérdida», más datos se descartan. Con frecuencia se suele aplicar un valor de pérdida entre 5 y 10, a veces hasta 50, sin degradar la imagen. El tamaño del fichero puede reducirse entre un 5 y un 40%. Con esto no podremos usar la opción de *Entrelazado* ni algoritmos de *Ruido* o *Tramado de motivo*. Para variar el ajuste entre los sectores seleccionados mediante un canal alfa, debemos hacer clic en el botón *Canal* que se encuentra junto al cuadro de texto *Pérdida*. En el cuadro de diálogo *Modificar ajuste de pérdida de calidad* seleccionamos un canal alfa del menú emergente, donde podremos establecer un rango de pérdida. El siguiente paso será seleccionar un algoritmo de reducción de color. Para especificar un número máximo de colores en la paleta, seleccionamos un número en el menú emergente *Colores*. Si la imagen contiene menos colores que el número especificado, la tabla de colores sólo tendrá el número de colores de la imagen. También podremos seleccionar la opción *Auto* al trabajar con una paleta de colores fija. Esta opción determina el número de colores de la tabla según la frecuencia de los mismos en la imagen. Es ideal para generar un número óptimo. Por otro lado, si la imagen contiene transparencias, podemos seleccionar *Transparencia* para preservarla o desmarcarla para rellenar con color mate parcial o totalmente los *pixels* transparentes. Además, si elegimos *Entrelazado* crearemos una imagen que se visualizará en versiones de baja resolución mientras el archivo de la imagen completa se descarga. Esto hace que el tiempo de descarga parezca más corto. Es un engaño muy sutil.

Cómo crear imágenes transparentes y mate

La transparencia hace posible colocar un objeto gráfico no rectangular como fondo de una página web. La transparencia de fondo, admitida por los formatos GIF y PNG, preserva los *pixels* transparentes de la imagen. Éstos permiten que el fondo de una página web se muestre en un navegador cualquiera. Los halos de fondo admitidos por los formatos GIF, PNG y JPEG representan la transparencia ya que rellenan o fusionan *pixels* transparentes con un color mate que se selecciona de forma que coincida con el fondo de la página web en la que se coloca la imagen. Los halos de fondo funcionan mejor si el fondo de la página web va a ser de un color uniforme y si conocemos el mismo ya de antemano. La imagen original debe contener *pixels* transparentes para poder crear transparencias de fondo o halos de fondo en la imagen optimizada. Podemos crear transparencias al crear una nueva capa. Cuando decimos que los formatos GIF y PNG-8 admiten un nivel de transparencia, estamos diciendo que los *pixels* pueden ser totalmente transparentes o totalmente opacos. Sin embargo, el formato PNG-24 admite transparencia a varios niveles, lo que permite preservar hasta 256 niveles de transparencia en una imagen.





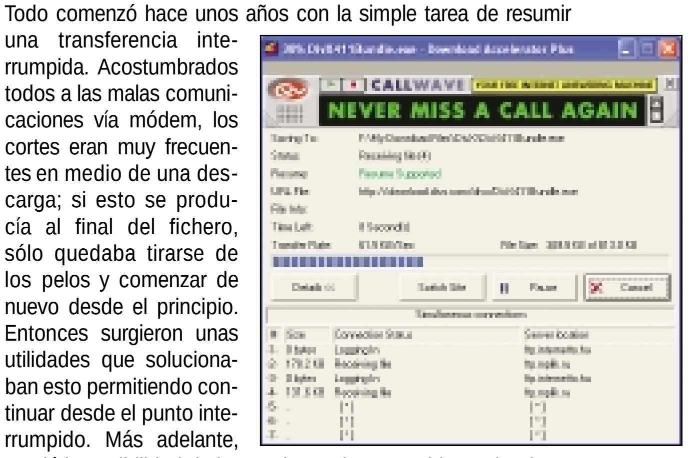
Optimiza la descarga de ficheros

Cómo aprovechar todas y cada una de las nuevas utilidades de descarga

Intermedio / 

Con las nuevas líneas de alta velocidad, la descarga de ficheros de gran tamaño está a la orden del día. Ahora es habitual «bajarse» cientos de «megas» y la velocidad es un parámetro crucial, con lo que cualquier software que pueda colaborar en este sentido es bienvenido. Muchas son las aplicaciones que pululan en el mercado pero pocas son las elegidas por los internautas.

Todo comenzó hace unos años con la simple tarea de resumir una transferencia interrumpida. Acostumbrados todos a las malas comunicaciones vía módem, los cortes eran muy frecuentes en medio de una descarga; si esto se producía al final del fichero, sólo quedaba tirarse de los pelos y comenzar de nuevo desde el principio. Entonces surgieron unas utilidades que solucionaban esto permitiendo continuar desde el punto interrumpido. Más adelante, surgió la posibilidad de buscar los mejores servidores donde se encontrara un fichero determinado. ¿Por qué conformarse con el servidor predeterminado cuando puede haber otros más rápidos?



La última innovación en llegar fue la segmentación en la descarga. Con la idea de ir más allá se pensó que, si había varios servidores buenos y capaces, al traernos el fichero de uno de ellos estábamos limitando nuestras capacidades. Dicho y hecho, en la actualidad la práctica habitual es la fragmentación del fichero, con lo que cada trocito se descarga desde un servidor diferente, de manera que la velocidad global de descarga aumenta. Veámoslo.

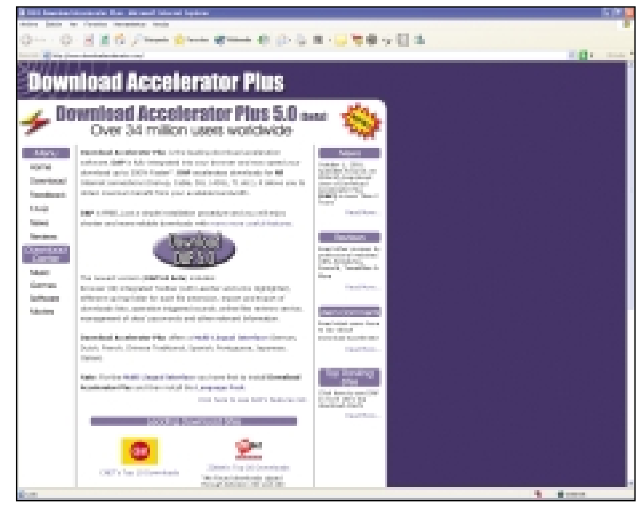
Download Accelerator

Este es uno de los programas de descarga más famosos. Se integra completamente en nuestro navegador y puede acelerar la descarga hasta en un 300%. Además, soporta cualquier tipo de conexión, como módem, cable, DSL, T1, etc. La idea es conseguir el mayor aprovechamiento de nuestro ancho de banda. A todo esto hay que añadir que Download Accelerator es gratuito. La versión más reciente, la 5.0, incluye numerosas características interesantes como una barra de herramientas integrada en el navegador, diferentes carpetas de almacén para cada tipo de fichero, importación y exportación de listas de descarga, sonidos personalizados, ficheros en línea y gestión de sitios con clave y contraseña. Por si esto fuera poco, también podemos incluir al paquete básico el soporte multilenguaje que incluye el castellano. Por último y durante la instalación, el programa nos interrogará por una serie de datos personales como edad, sexo, profesión e intereses. Contestar será totalmente opcional.

Paso 1

Toma de contacto

Después de instalar Download Accelerator, se activará automáticamente cuando efectuemos la descarga de ficheros EXE, ZIP, MP3, ARJ, RAR, LZH, Z, GZ, GZIP, TAR, BIN, AVI, MPG, etc. Podremos cancelar la descarga en cualquier momento para terminarla más tarde. También soporta características de «arrastrar y soltar» e incluso la inserción de una URL directamente. Si perdemos la conexión, no tendremos por qué preocuparnos; una vez reestablecida, podremos continuar con el fichero «colgado» como si nada hubiera pasado. Las caracte-

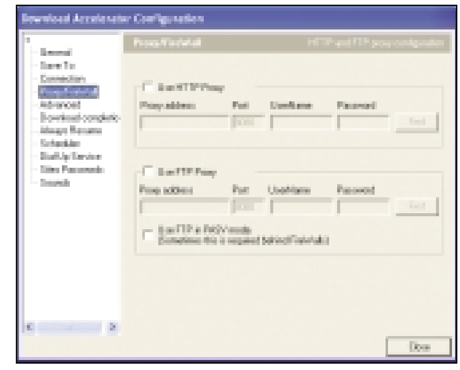


rísticas de aceleración y resumen sólo funcionan cuando nos «bajamos» un fichero de un servidor que soporta este tipo de opciones. Esto no pasa con servidores antiguos, que, afortunadamente, son cada vez menos. También es posible que, si estamos usando un servidor *proxy*, éste sea el culpable de que no podamos «resumir» o acelerar una descarga.

Paso 2
«Resumen» de descargas

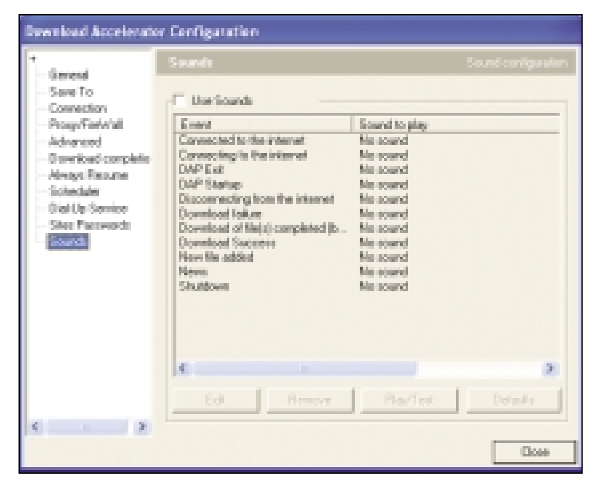
Intermedio

Una interesante característica de DAP (*Download Accelerator Plus*) es el *Always Resume*, opción que nos permitirá «resumir» transferencias de ficheros interrumpidas incluso desde servidores que no admitan esta característica. Hasta hoy, cuando comenzábamos una descarga desde un servidor y por alguna razón la transferencia se interrumpía, necesitábamos empezar la descarga desde el principio. Sin embargo esto se ha acabado. Ahora podemos continuar esas transferencias interrumpidas siempre que tengamos un módem y que el fichero no supere los 10 Mbytes. En cuanto al soporte de *proxies*, Download Accelerator los soporta tanto en su versión HTTP como FTP. Para definir uno debemos ir a *Proxy/Firewall* en la pantalla de configuración. En este punto hay que recordar también que muchos *proxies* antiguos no soportan ni «resumen» ni aceleración de ficheros.



Paso 3
Configuración del programa

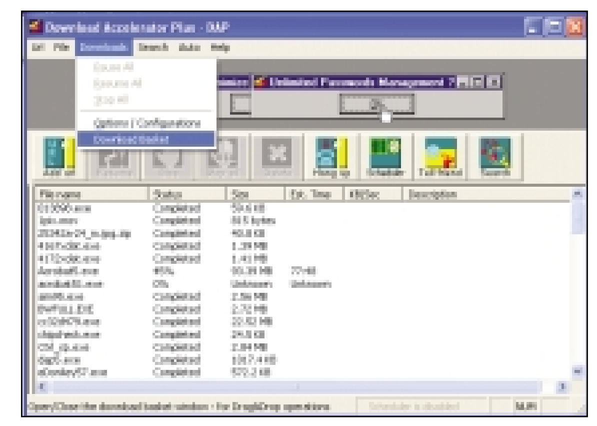
La integración a nivel de navegador es total con las versiones Internet Explorer 4.x/5.x y Netscape 4.x (la versión 6.x no se soporta aún). También pueden emplearse otros navegadores diferentes con Download Accelerator, pero la integración no será total. Seremos capaces de usar las características de «arrastrar y soltar» o incluso entrar la dirección URL directamente. En cuanto a la configuración del programa, toda se centraliza en la pantalla *Configuration* a la que llegaremos a través de *Downloads/Options/Configuration*. Allí tendremos



cuatro secciones. *General*, *Connection*, *Proxy/Firewall* y *Advance*. En cuanto al «resumen» de descargas interrumpidas, el proceso es muy sencillo. Tan sólo tenemos que buscar el fichero deseado en la lista de la ventana principal del programa y, si tenemos conexión y hay servidores disponibles, continuará donde se había interrumpido.

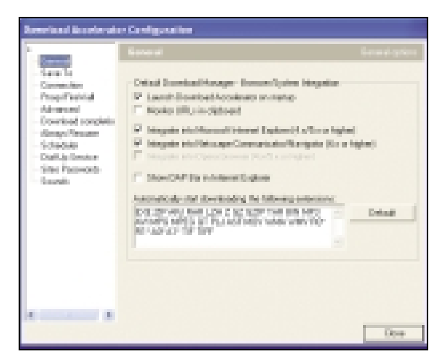
Paso 4
Cómo «arrastrar y soltar» y los servidores espejo

Para «arrastrar y soltar» debemos posicionarnos en el menú *Downloads* y dentro de él dirigirnos a *Download Basket*. Una pequeña ventana se abrirá automáticamente y permanecerá en nuestro escritorio mientras que Download Accelerator permanezca abierto. En cualquier momento podremos «arrastrar» enlaces a esta particular «cesta» desde nuestro navegador para finalmente soltarlos allí. Inmediatamente se abrirá la ventana de descarga y se iniciará el proceso de transferencia. En cuanto a la característica de servidores espejo o *mirror*, está plenamente soportado por esta herramienta. La idea es buscar el fichero que queramos en varios servidores para encontrar el que tenga más rendimiento. Una vez confeccionada la lista de los mejores, Download Accelerator procederá a descargar porciones del mismo de los más rápidos. Si nos fijamos bien durante la descarga, veremos un botón que indica *Details*. Allí podremos encontrar información más detallada sobre el



proceso de descarga, así como la transferencia de cada porción individual del fichero que nos estemos descargando («bajando»). Si solamente vemos una conexión, esto implicará que la aceleración no está disponible en este momento, ya sea por culpa de nuestro *proxy* o por el servidor en cuestión.

Paso 5
Desactivación del software



Si estamos usando algún software de descarga alternativo, es posible que esto interfiera en el correcto funcionamiento de Download Accelerator. Para reactivar la integración del mismo, debemos dirigirnos a la ventana de configuración y allí en la sección *General* activar la casilla *Browser Integration*. Luego deberemos reiniciar el navegador para

que los cambios surtan efecto. Pero, ¿qué ocurre si queremos desactivar temporalmente esta utilidad? Muy fácil, tan sólo tendremos que mantener pulsada la tecla «Alt» mientras hacemos clic en el fichero que deseemos descargar. En este mismo sentido, si encontramos algún fichero con una extensión que no esté soportada por defecto, podemos añadirla sin ningún problema si presionamos las teclas «Alt» y «Ctrl» mientras hacemos clic.

El más usado

Merece la pena que hagamos un alto en el camino para analizar por qué Download Accelerator es unos de los programas de descarga de ficheros más utilizado: ya en octubre de 2001 se anunció la cifra de 30 millones de usuarios registrados en todo el mundo. Se trata de una plataforma para la distribución de contenido multimedia a través de Internet; Download Accelerator mejora la descarga de software, música, juegos, películas y vídeos en la Web, acelerando el proceso entre un 200 y un 400%. Una de las claves para su rápida difusión ha sido el «boca a boca» entre amigos y compañeros del trabajo. La base de usuarios es tan enorme, que se calculan entre 8 y 9 millones de descargas diarias, que han acumulado un total de 3 billones desde que salió al mercado. El secreto del éxito lo tiene en parte su novedoso funcionamiento. Primero busca los sitios de descarga donde se encuentra el archivo, luego escoge los mejores según la configuración del cliente. El chequeo se hace en tiempo real para después conectarse a varios de estos sitios para comenzar la descarga en porciones. Esto permite un balance de carga muy equilibrado entre varios servidores de todo el mundo y reduce el tiempo de descarga, aprovechando al máximo el ancho de banda disponible. Detrás de esta popular herramienta se encuentra SpeedBit, empresa fundada en 1999 y que tiene su cuartel general en Israel.

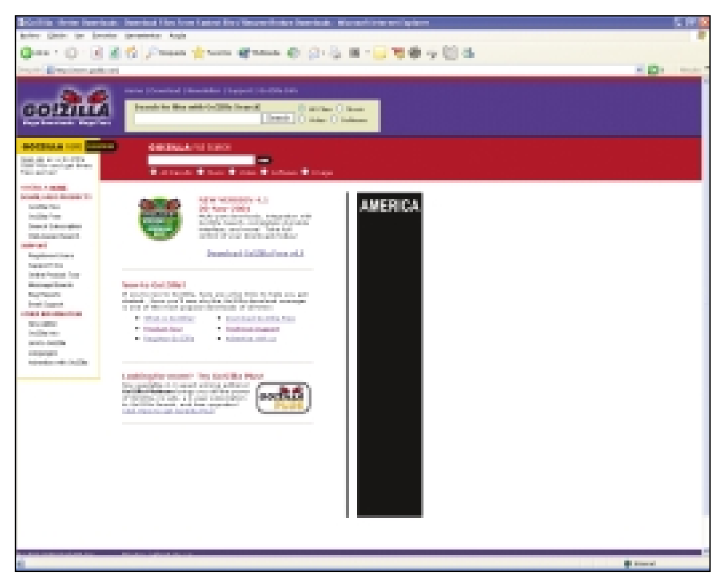
Go!Zilla

Al instalar el programa, se nos ofrece la posibilidad de elegir fuentes pequeñas (predeterminadas) y fuentes grandes. En el siguiente punto debemos escoger *Novice User* (opción predeterminada, recomendado para usuarios noveles que tengan poca experiencia en descargar ficheros) o *Advanced User* (para usuarios experimentados con Go!Zilla (*www.gozilla.com*) o descargando ficheros; idóneo para manejar un gran volumen de descargas, monitorizarlas y ajustar ciertos valores para optimizar el rendimiento). Otra opción para configurar es también la posibilidad de que no aparezca una ventana por cada descarga.

Hay que tener en cuenta que una de las causas por las cuales Go!Zilla es gratuito es por la inclusión de ciertos programas parásitos en su instalación. Se trata de una opción por defecto, aunque podemos negarnos. En este caso se nos intentan colar los famosos Gator (recuerda todas nuestras contraseñas y datos para rellenar automáticamente formularios y demás registros) y OfferCompanion (ofertas e información diversa). Nuestra recomendación es que no los instaléis. El primero recuerda todas nuestras contraseñas y ha habido rumores de filtraciones de información a terceros con clientes de este programa. El segundo es un montón de publicidad embutida bastante molesto.

Por último, se procede a instalar la herramienta eZula TopText iLookup 2.0, que es un compendio de diccionario, buscador, enciclopedia en línea y varias cosas más con la idea de simplificarnos la navegación. Para finalizar, sólo queda decidir si instalamos un *plug-in* para nuestro navegador, denominado *Clickguide,* que integra Go!Zilla con nuestro explorador de Internet para que podamos buscar ficheros (información útil, motores de búsqueda, tiempo local, películas, programas de TV y más) sin abandonar el mismo. El último paso de la instalación consiste en configurar una serie de valores importantes: primero la velocidad de conexión: módem, RDSI, ADSL, cable, red u otras. Después tendremos que reiniciar para que los cambios surtan efecto.

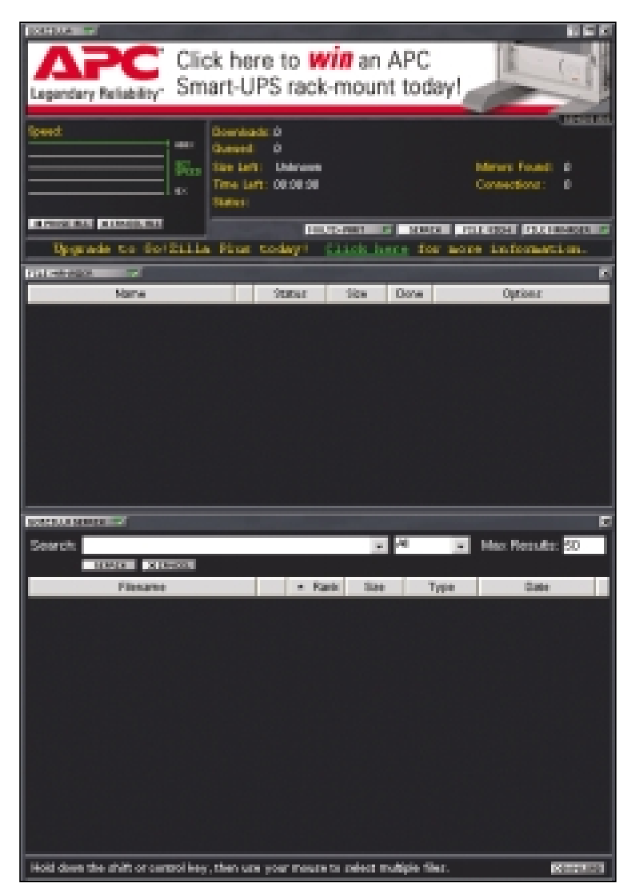
Paso 1
Enlaces eficientes



La manera más fácil de «arrastrar y soltar» ficheros dentro de Go!Zilla es que aparezca siempre visible en la parte superior de nuestro navegador. Esto lo podemos lograr de dos formas, usando la característica *On top* o *Drop target*. Luego, deberemos hacer clic y arrastrar el enlace del fichero que queremos descargar a la ventana de Go!Zilla. Si aparece una «X» dentro de un círculo, significará que no es un vínculo de fichero válido. Esto es debido a que el enlace que intentamos arrastrar tiene el acceso a través de una imagen o fichero y nuestro navegador cree que intentamos arrastrar sólo la imagen, y no el enlace. A partir de la versión 4.0 de Internet Explorer ya se ha solucionado este problema. Si usamos una versión antigua de este navegador o Netscape o cualquiera que no soporte correctamente esta funcionalidad, aún nos queda un truco que utilizar. Nos referimos a *cortar y pegar*. Primero hacemos clic con el botón derecho en el enlace y seleccionamos *Copy*. Después nos vamos a Go!Zilla y elegimos *Paste*. Entonces, el enlace será añadido a la lista de ficheros.

Paso 2
Vicisitudes de la descarga

Cuando obtenemos un mensaje de error al intentar descargar un fichero, puede deberse a varias razones: acceso no autorizado, errores de red e incluso una sobrecarga en el número de personas en el servidor de ficheros en ese momento, lo que nos indicaría que probáramos más ade-

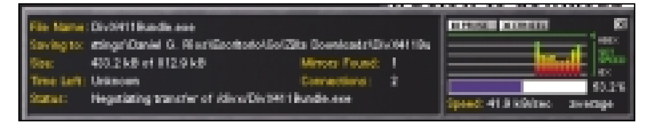


lante. Podemos ver un mensaje de error detallado en el monitor del estado del fichero. Go!Zilla intentará traerse de nuevo el fichero el número de veces que hayamos estipulado en el campo *Retry attemps* que se encuentra en *Go!menu/Options transfer*. Si hemos descargado parcialmente un fichero Go!Zilla, comenzará con él en el punto donde abandonamos la descarga una vez que reanudemos la conexión. Si esta característica no puede usarse, una posible causa será que estamos utilizando un servidor *proxy* para conectarnos a Internet y éste no soporta el «resumen» de archivos. Si por el contrario podemos «resumir» unas descargas sí y otras no, entonces el problema no es nuestro servidor *proxy*, es debido a que el servidor donde se encuentra situado el fichero no soporta esta característica. A medida que pasa el tiempo, más y más servidores la soportan, por lo que esta situación es cada vez más rara. Go!Zilla permite «resumir» ficheros tanto desde HTTP como de FTP.

Paso 3

El sitio más rápido

Cuando nos bajamos un fichero con Go!Zilla, el programa lo busca a través de FTP para tratar de localizar sitios adicionales que también tengan el fichero (también denominados sitios espejo). A veces, hay un sitio más cercano a nosotros o simplemente más rápido que el que hemos elegido por defecto. Go!Zilla encuentra para nosotros automáticamente

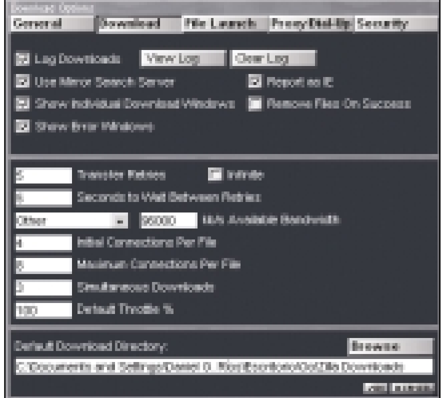


estos lugares si tenemos activada la opción *Go!Zilla Mirror Search Service* que se encuentra en *Menu/Options/World Wide Mirror Search* y que rápidamente chequea cada sitio antes de una descarga para ver si está operativo y cuál es el más rápido. Si durante este proceso recibimos un mensaje que ponga algo así como *Unable to connect to...* significará que el motor de búsqueda FTP está caído momentáneamente o que tiene una respuesta muy lenta. Una opción entonces es probar a incrementar el tiempo de búsqueda en *Menu/Options/Connection* o cambiar el tipo de motor de búsqueda en *Menu/Options/FTP Search*. Pero, ¿qué ocurre si queremos realizar la descarga desde un sitio en particular de nuestra elección? La solución es sencilla: tan sólo tendremos que acceder a las propiedades del fichero a través del botón derecho del ratón y allí veremos una lista de los sitios donde se ha localizado. Elegiremos el que queramos y haremos clic para comenzar la descarga desde ese lugar en particular.

Paso 4

Descargas alternativas

Podemos decirle a Go!Zilla (*Options/Transfer/Maximum Simultaneous Transfers*) cuántos ficheros queremos descargar como máximo a la vez. El número por defecto es dos, pero si cambiamos este valor a uno, Go!Zilla se bajará cualquier fichero que hayamos seleccionado, uno a uno, en un único fichero. Para comenzar la descarga de un grupo de ficheros a una hora determinada, debemos seleccionar primero los ficheros deseados y luego hacer clic en el botón *Schedule* y rellenarlo con la hora determinada. Otra cuestión diferente es hacer que Go!Zilla consiga descargar ficheros de sitios protegidos con contraseña. El lugar indicado para efectuar los arreglos es *Options/Security*, donde podremos añadir un sitio determinado y asignarle un nombre y una contraseña. Por otro lado, un problema que nos puede surgir es que la optimización de sitios de Go!Zilla conmute de uno a otro con demasiada asiduidad. Entonces deberemos dirigirnos a *Options/Transfer* para establecer la velocidad mínima de conmutación entre sitios. Si la transferencia sostenida en las descargas disminuye por debajo de nuestro umbral, entonces Go!Zilla buscará un nuevo sitio con más calidad al que migrar. Si estos cambios se producen con mucha frecuencia, podremos poner en esta sección un valor alto más permisivo.

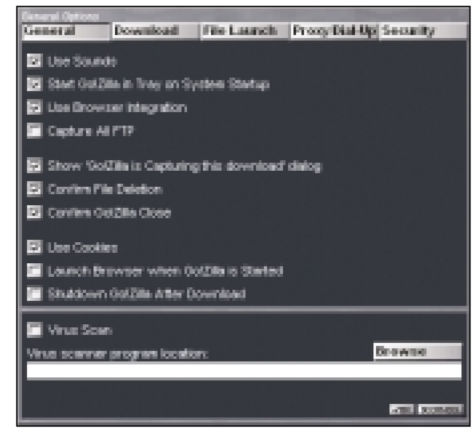


Paso 5

Opciones avanzadas

En muchas ocasiones, puede ser muy útil desactivar Go!Zilla para un fichero determinado o para un sitio en concreto. Para ello sólo tenemos que mantener pulsada la tecla «Alt» mientras hacemos clic en el enlace. Si queremos desactivarlo por un periodo de tiempo más largo, podemos acudir a *Auto* y apagar la integración con el navegador o incluso la captura de sitios FTP. Si lo que queremos es desactivar por completo la aplicación, una alternativa es desinstalarlo por comple-

to. En cuanto a sitios seguros, Go!Zilla no soporta los lugares seguros del tipo HTTPs que utilizan encriptación y técnicas similares. Así pues, también ocurre lo mismo con los sitios que emplean llamadas de redireccionamiento que «despistan» a Go!Zilla impidiéndole encontrar el más adecuado. En otro orden de cosas, si por cualquier causa esta herramienta no es capaz de capturar ciertas descargas, debemos cerciorarnos de dos cosas: una, que esté activada la integración con el navegador, y otra, que la causa se deba posiblemente a un enlace redirigido que impide a Go!Zilla realizar bien su tarea. Lo mejor en este caso es que arrastremos el enlace a la ventana principal del programa o que hagamos un «copiar y pegar».



Descargar ficheros con Go!Zilla

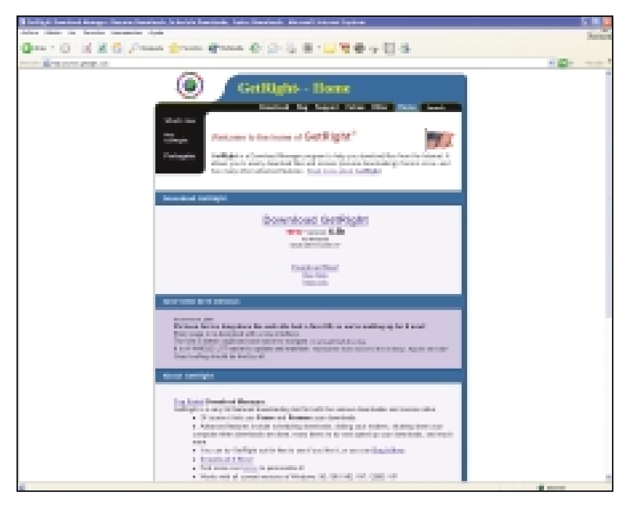
Veamos con esta utilidad un caso práctico de descarga. Una vez que hemos hecho clic en el fichero que queremos descargar y se arranca el interfaz predeterminado, «empieza la fiesta». Lo primero que tendremos que hacer será seleccionar un directorio de destino para el archivo. Por defecto se guardan en *Go!Zilla Downloads* que es una carpeta localizada en nuestro escritorio desde el momento de la instalación. Como podemos ver, tenemos varias alternativas. Una de ellas es *Download Now* que es la más habitual y es el camino más rápido para comenzar la descarga. *Download Later* nos permite aplazar la bajada del archivo para planificarlo posteriormente. Si por cualquier razón no queremos que *Go!Zilla* maneje este archivo, debemos seleccionar la opción *Bypass. Go!Zilla*. Esto es útil si queremos ver el formato nativo del fichero o si queremos que el navegador procese el fichero de forma estándar.

GetRight

Este programa shareware, (*www.getright.com*) no sólo ayuda a descargar ficheros sino que también soporta «resumen» de descargas interrumpidas, descarga más rápida gracias al uso de segmentos, planificación del trabajo y otras características avanzadas. Al igual que pasa con Go!Zilla, también viene de serie con los programas Gator y OfferCompanion. El primero recuerda nuestras claves y las escribe por nosotros y el segundo nos bombardea con ofertas y promociones. Recomendamos no instalarlos. También durante la instalación se nos da a elegir el tipo *Easy* con los valores más comunes por defecto y el *Custom* donde podremos cambiar las opciones a nuestro gusto.

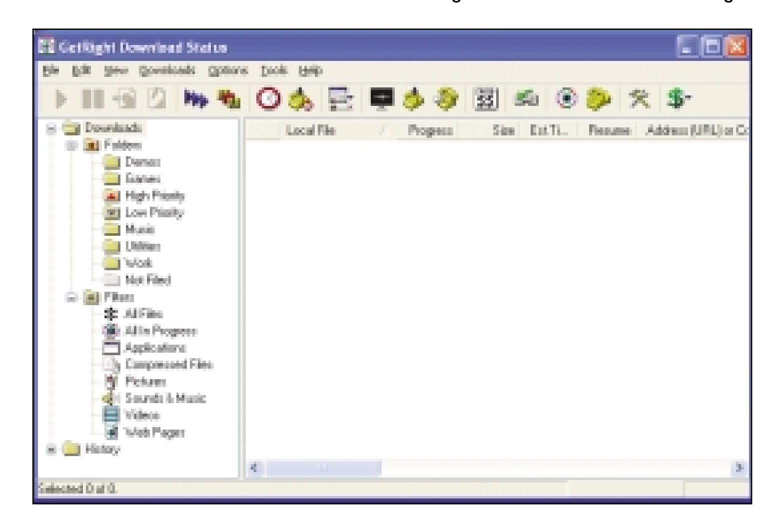
Paso 1
Más aceleración

Hay muchas maneras de encontrar un sitio espejo donde buscar el fichero que queremos. GetRight calcula automáticamente los *mirror* para muchos sitios populares (como Tucows). También es posible usar la búsqueda FTP para encontrar más localizaciones para un fichero. Debemos hacer clic en el botón *Options* cuando un fichero se está descargando y seleccionar *Search for Alternates* en el menú correspondiente. O si el sitio donde hemos encontrado el fichero tiene un listado de varios *mirrors*, sólo tenemos que seleccionar unos pocos para que GetRight los adopte. Una regla básica para saber qué servidor es más rápido es fijarnos en la distancia. Cuanto más cerca esté de nuestra ubicación, mejor. Por otro lado, GetRight automáticamente hará *ping* a cada uno para ver cuál es el más rápido y conmutará la descarga a ese.



Paso 2
Descarga segmentada

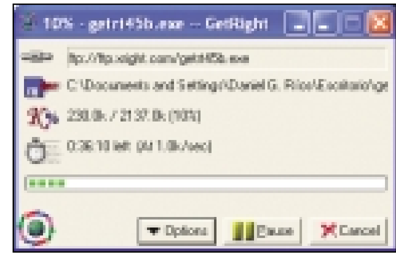
Segmentar un fichero permite a GetRight descargarse diferentes partes del mismo a la vez. Por ejemplo, un fichero se divide en dos partes y la primera la cogemos del servidor A y la segunda del B. Dependiendo de nuestra conexión a Internet, esto puede mejorar increíblemente la velocidad de descarga. Podemos usar hasta ocho segmentos. Para decirle a GetRight



que queremos transferencias segmentadas, debemos ir al menú *Options* cuando se descarga un fichero y seleccionar *Segmented Downloading* y el número de segmentos que queremos utilizar. También podemos hacer que esta sea la opción por defecto en el menú *Configuration*.

Paso 3

Descarga controlada

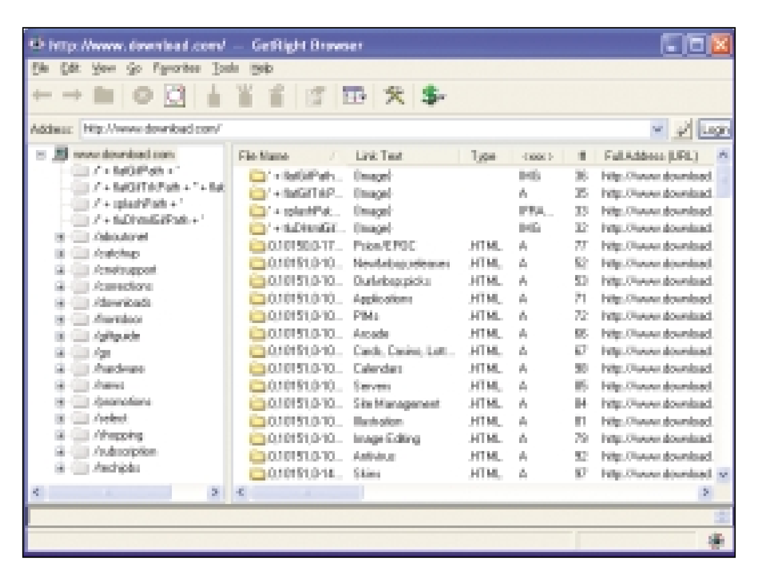


Algunos sitios usan URLs que GetRight y programas similares piensan que son ficheros, por lo que trata de descargarlos. Cuando GetRight está integrado en el navegador Web, si mantenemos pulsada la tecla «Shift» mientras hacemos clic en un enlace, GetRight no intentará bajarse el enlace. También, si mantenemos pulsadas las teclas «Ctrl» y «Alt» en las mismas circunstancias, GetRight intentará obtener el enlace como sea, incluso si es uno típico de navegador Web, como HTML. También tenemos la opción de crear una lista de servidores que siempre serán ignorados. ¿Y cómo creamos una lista de ficheros para descargar? GetRight acepta dos formatos diferentes, LST o URLS. Una vez hayamos creado uno de ellos, podemos usar el comando *GETRIGHT NombreListaFicheros* para importar la lista de ficheros para descargar.

Paso 4

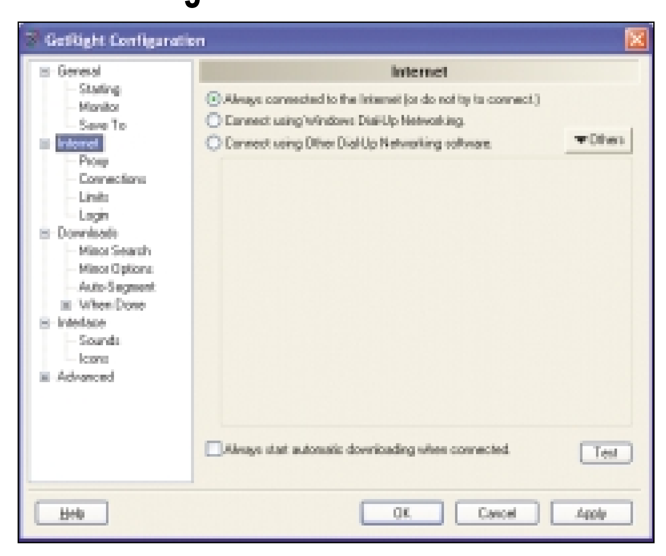
Ficheros que se resisten

Una opción muy curiosa es la de descargar todos los ficheros de una página Web determinada. Dentro del menú *Tools*, tenemos el elemento *GetRight browser* que nos permite explorar sitios FTP o páginas Web y fácilmente añadir ficheros para descargar. Si por el contrario nuestro problema es que queremos bajar archivos que requieren nombre y contraseña, podemos configurar esto para cada servidor particular que sea necesario en la página *Login Configuration*. Allí podremos establecer el nombre y la clave de cualquier descarga que realicemos. Debemos ir a *Change Username and Password* en el menú *Advanced*.



Paso 5

Recuperar un fichero parcialmente descargado



Si queremos que GetRight resuma una descarga cuando nos conectemos a Internet, debemos ir a la página de configuración de Internet y seleccionar *Always start automatic downloading when connected*. Si estamos usando un módem, esto puede causar que nuestro software de red intente conectarse a Internet cuando GetRight mire a ver si estamos conectados. Hay que asegurarse de que el botón de *Test* no esté activado cuando no estemos conectados para evitar que nuestro PC intente hacerlo. Por otro lado, podemos incluso finalizar un archivo parcialmente descargado con otro programa de descarga. Para ello debemos localizar el «trozo» perdido con extensión TMP e ir inmediatamente a *Advanced Menu*, *Recover Lost Downloads*. Seleccionaremos el fichero en cuestión e indicaremos la URL del servidor.

GetRight versión 4.5

Shareware o Adware: ahora los usuarios no registrados tienen estas dos posibilidades para elegir.

Download History: un árbol con el estado de la descarga donde podremos encontrar fácilmente los ficheros descargados. También podremos ver el tiempo transcurrido y la velocidad media.

Filemirrors.com: *Mirror* de GetRight para buscar ficheros de forma anónima entre otros usuarios que los comparten.

Mirror Manager: gran mejora para añadir, controlar y verificar nuestros servidores para una descarga.

Reorganizar la configuración: para usar una estructura de árbol.

Verify: ahora se puede chequear los enlaces en la pantalla de estado.

SOCKS: en esta versión también soporta este tipo de *proxies*. Se ha añadido al marcador para hacerlo mejor con diferentes ISPs y con distintos nombres de usuario y parámetros del *proxy*.



Listas de Correo

Participa, opina, discute y comparte a través de tu correo electrónico

Intermedio

Las listas de correo guardan un cierto parecido con los foros de noticias, permitiendo a los usuarios crear y participar en comunidades con intereses específicos. Ambos servicios permiten intercambiar mensajes con gente de gustos similares. En las listas de correo los mensajes nos llegan a nuestro *e-mail* en lugar de estar esperándonos en un foro común. Esto permite que haya menos mensajes sin sentido, pues uno revela su dirección verdadera de correo electrónico al suscribirse. Tanto en las listas de correo como en los *newsgroups* el principal objetivo es la participación de sus miembros para hablar de los temas permitidos, compartir conocimientos, dudas, contestarlas, hacer comentarios, dar opiniones, anunciar eventos, etc. Una lista de correo es una forma de fomentar la discusión grupal sobre los temas que nos interesan, para que todos podamos hablar sobre ellos y resolver nuestras dudas. Su funcionamiento se basa en que todo mensaje enviado a la lista es reenviado a cada una de las personas inscritas.



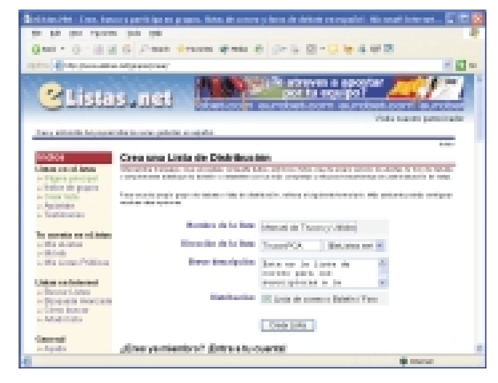
Crear y administrar una lista de correo

Paso 1

Crear un lista de correo

Para crear nuestra propia lista de correo, utilizaremos el servicio *eListas.net*, que además de ser totalmente gratuito, funciona en español. Introduciremos la dirección *www.eListas.net* en nuestro navegador y completaremos el formulario existente en la página principal. Para ello necesitaremos:

Nombre de la lista: aquí escribiremos el título bajo el cual figurará nuestra lista en el buscador y en los correos electrónicos, por ejemplo: «Mis amigos», «Todo sobre Trucos», «Informática para novatos», etc.



Dirección de la lista: en este campo insertaremos el nombre de la dirección electrónica que tendrá nuestra comunidad. Tendremos en cuenta no usar espacios en blanco, la letra «ñ», acentos, apóstrofes y otros símbolos. La dirección de la lista ha de ser breve y fácilmente reconocible ya que será la dirección a la que los suscriptores deberán enviar sus mensajes.

Breve descripción: en este espacio escribiremos las características de nuestra lista de correo. El texto que introduzcamos en este campo será el que se hará público para identificar nuestra comunidad cuando se efectúe una búsqueda.

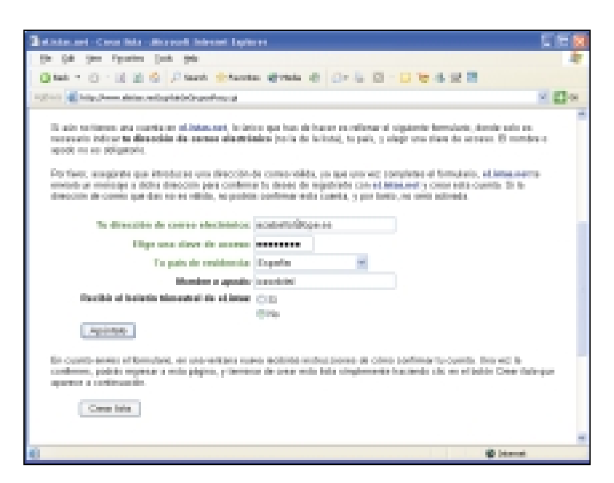
Distribución: aquí seleccionaremos entre *Lista de correo* o *Boletín/Foro*. Básicamente la diferencia radica en que los suscriptores puedan enviar mensajes (Boletín/Foro) iniciando discusiones e intercambio opiniones o simplemente pueda hacerlo el titular de la misma (lista de correo).

Paso 2

Darnos de alta como usuario de eListas

Tras pulsar el botón *Crear lista* aparecerá una nueva ventana en la que tendremos que configurar el acceso a la misma, que nos permitirá su administración en el futuro en caso necesario. Para ello hemos de crear una cuenta en *eListas.net*, que realizaremos rellenando el formulario existente en la parte inferior de la misma página.

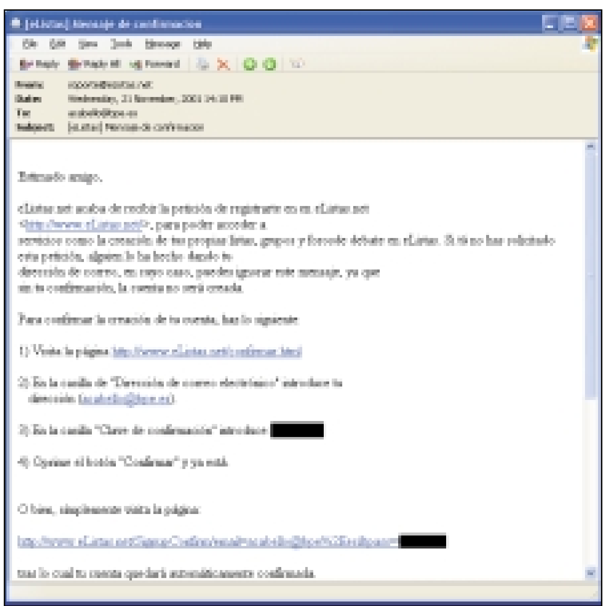
Tu dirección de correo electrónico: introduciremos nuestra cuenta habitual de correo electrónico que será la que nos identificará como propietario y administrador de la lista de correo. Resulta importante asegurarnos de introducir una dirección de correo válida, ya que a esa dirección se enviará la



confirmación de registro para la creación de la cuenta. Si no introducimos una dirección válida de correo, no podremos confirmar esa cuenta y por tanto no podrá ser creada.
Elige una clave de acceso: en este campo insertaremos una contraseña que autenticará nuestra identidad.
Tu País de residencia: este campo es obligatorio, si bien únicamente es utilizado para funciones estadísticas del sistema.
Nombre o apodo: opcionalmente podemos introducir nuestro nombre o apodo. Este nombre aparecerá cuando enviemos correo a través de la lista de correo, junto con el nombre de la propia lista, siguiendo la sintaxis: apodo (nombre_de_la_lista)

Paso 3
Confirmar nuestra cuenta

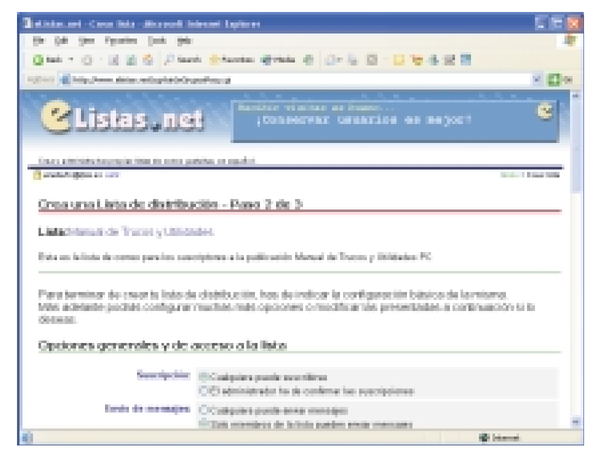
Sin cerrar esta misma página, a la que volveremos para finalizar la creación de nuestra cuenta, pulsaremos sobre el botón *Apúntate*. Nuestra inscripción será formulada y se enviará, a la dirección de correo especificada, un correo electrónico de confirmación, con las instrucciones necesarias para finalizar la creación de nuestra lista de correo. En estas instrucciones se incluye una clave que tendremos que introducir en la dirección *www.eListas.net/confirmar.html* junto con nuestra dirección de correo electrónico. Una vez confirmada la creación de nuestra cuenta, ya podremos gestionar nuestra lista de correo así como crear nuevas y encargarnos de nuestras propias sus-



cripciones. A estas opciones se accede desde la página *Mis eListas.* Sin embargo, volveremos a la página que anteriormente hemos dejado abierta para pulsar el botón *Crear lista.*

Paso 4
Finalizar la configuración

Para terminar de crear nuestra lista de distribución, indicaremos la configuración básica de la misma, si bien más adelante tendremos la posibilidad de configurar muchas más opciones que iremos viendo a lo largo del texto. Una de las más importantes es la de *Suscripción:* dependiendo de la configuración que escojamos, cualquiera podrá suscribirse a nuestra lista de correo o cada suscriptor tendrá que ser «aprobado» por el dueño de la lista antes de poder formar parte de ella. Aunque eso signifique más trabajo para el dueño de la lista que tiene que «aprobar» a cada persona suscrita, nuestra lista



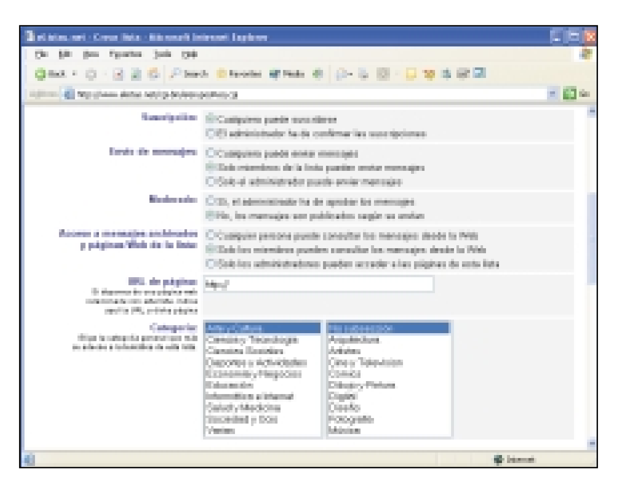
estará protegida contra molestias externas, ya que existe el problema generalizado de que las listas no restringidas son «atacadas» por bromistas que envían mensajes sin sentido y en ocasiones molestos. Sin embargo, cuando una lista de correo crece en tamaño, es difícil conocer a todas las personas suscritas, y así su aprobación se convierte en una mera formalidad. La principal ventaja de una lista restringida es que el dueño de la lista puede anular la suscripción de alguien que constantemente se salte las reglas fijadas por los miembros de la lista.

Paso 5
Envío de mensajes

Bajo este apartado, determinaremos si cualquier usuario de Internet podrá enviar mensajes a la lista de correo que vamos a crear o si, por el contrario, únicamente los miembros de la lista podrán enviar mensajes. De nuevo, escoger la segunda alternativa es la más recomendable. Si seleccionamos la opción *Sólo el administrador puede enviar mensajes*, nuestra comunidad se convertirá en un *Boletín* en el cual la porción de los suscriptores será nula y se dedicarán únicamente a recibir y leer los mensajes que el administrador envíe.

Paso 6
Listas moderadas

Bajo el apartado *Moderado* debemos escoger el tipo de comunidad que implementaremos para nuestra lista de correo: *Moderada* significará que los mensajes deberán ser aproba-



dos por el administrador antes de ser publicados y reenviados al resto de usuarios; o bien *No moderada*, en ella los mensajes se publicarán inmediatamente después de ser enviados por los miembros de la comunidad sin necesidad alguna de aprobación por parte del administrador. Escoger la primera opción representará una gran cantidad de trabajo para el dueño de la lista, sobre todo si se trata de una lista muy activa. La aprobación se usa como forma de controlar los tipos de mensajes que pasan a la lista. Un ejemplo en que se usa la moderación es en una lista del tipo «boletín de noticias», donde necesitaremos asegurarnos que cada mensaje provenga de una fuente autorizada. En la medida en que nuestro grupo tenga claro el propósito de la lista y el modo en que funciona, y si se trata de una lista que ya es «restringida», es recomendable no configurarla como *No moderada*. Únicamente moderaremos la lista si encontramos necesario mantener un control estricto de lo que se envía. Esto, de todos modos, no significa anarquía absoluta: cualquier miembro que, a juicio del administrador de la lista o de los otros miembros, se esté comportando inadecuadamente, podrá ser expulsado.

Paso 7

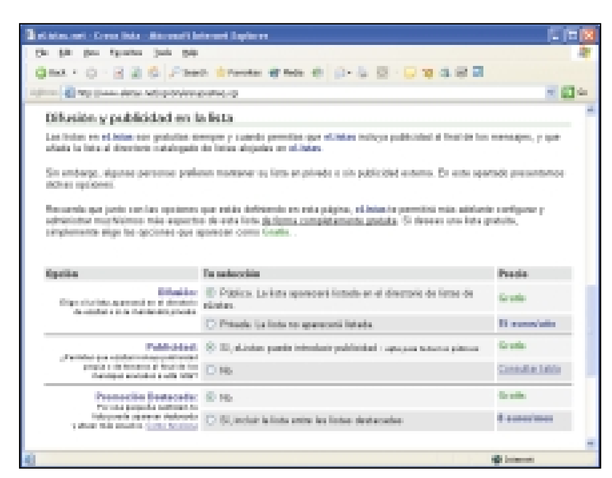
Otras opciones

Existen otros apartados que deberemos configurar como el *Acceso a mensajes archivados y páginas web de la lista*. Una vez más, dependiendo del nivel de privacidad con el que deseemos dotar a nuestra lista de correo, seleccionaremos (de menor nivel de seguridad a mayor) *Cualquier persona puede consultar los mensajes desde la web, Sólo los miembros pueden consultar los mensajes desde la web* o *Sólo los administradores pueden acceder a las paginas de esta lista*. Bajo el apartado *URL de página*, introduciremos la dirección de la página web relacionada con el grupo de usuarios de la lista. Por último, en el apartado *Categoría*, ubicaremos en una determinada categoría nuestra comunidad según los temas que vaya a tratar. Tendremos en cuenta que, cuanto mejor ubiquemos nuestra lista de correo, más sencillo será encontrar nuestra comunidad.

Paso 8

Sufragar los gastos

Bajo el tercer apartado principal *Difusión y publicidad en la lista*, se encuentran una serie de opciones que podremos configurar dependiendo si queremos mantener nuestra lista de correo privada de forma que no aparezca en el directorio principal de eListas, sin publicidad externa que eListas incluye por

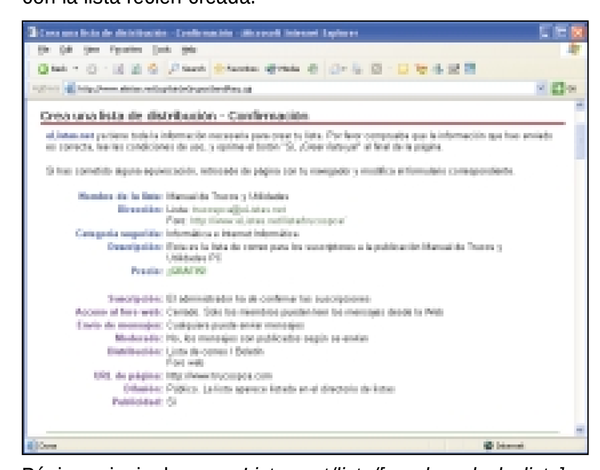


defecto al final de los mensajes, con el fin de sufragar los gastos propios de la lista de correo; o bien, si queremos anunciar nuestra lista para atraer una mayor cantidad de usuarios. Dentro de los apartados *Difusión, Publicidad* y *Promoción destacada* optar por la segunda opción significará pagar una pequeña cuota que dependerá de los servicios escogidos.

Paso 9

Confirmación y resumen de configuración

Una vez configurada por completo nuestra lista de correo, se desplegará un página que resumirá todas las opciones de configuración que hemos realizado y todavía permitirá, en caso necesario, volver atrás para corregir los posibles errores. Si todo está correcto, aceptaremos los términos de las condiciones de uso y pulsaremos una única vez sobre el botón *Sí. ¡Crear lista ya!*. Finalizado todo el proceso, que no lleva más de 10 minutos, aparecerá una pantalla donde deberemos tomar nota de las páginas y direcciones importantes relacionadas con la lista recién creada.



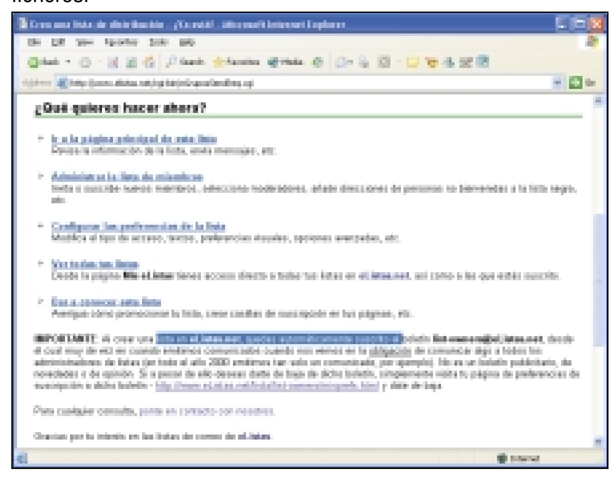
Página principal: *www.eListas.net/lista/[nombre_de_la_lista]*
Para enviar mensajes a la lista: *[nombre_de_la_lista]@eListas.net*
Para darse de alta: *[nombre_de_la_lista]-alta@eListas.net* o *www.eListas.net/lista/[nombre_de_la_lista]/alta*
Para darse de baja: *[nombre_de_la_lista]-baja@eListas.net* o *www.eListas.net/lista/[nombre_de_la_lista]/baja*
Para administrar la lista: *www.eListas.net/lista/[nombre_de_la_lista]/admin*
Otras direcciones: *[nombre_de_la_lista]-info@eListas.net*; *[nombre_de_la_lista]-faq@eListas.net*

Paso 10
Otras alternativas

En la misma página, bajo el resumen de las direcciones de nuestra lista, encontramos varios enlaces que nos permitirán ahora o en el futuro administrar y configurar nuestra lista. Estas opciones y otras importantes son:

Ir a la página principal de esta lista (*www.eListas.net/lista/[nombre_de_la_lista]*)

En esta página podremos revisar la información de la lista, cuándo fue creada, el número de miembros, la categoría, descripción y sus características, enviar mensajes, así como también crear encuestas, informar de eventos o intercambiar ficheros.



Administrar la lista de miembros (*www.eListas.net/lista/[nombre_de_la_lista]/admin/miembros.html*)

Desde esta página, veremos un listado completo de los usuarios de nuestra lista de correo, y tendremos la posibilidad de invitar, suscribir o eliminar miembros, añadir moderadores o direcciones de personas, que no podrán suscribirse a nuestra lista, al listado negro de usuarios, etc.

Configurar las preferencias de la lista (*www.eListas.net/lista/[nombre_de_la_lista]/admin.*)

Desde aquí podremos modificar el tipo de acceso a la lista de correo, textos, preferencias visuales, opciones avanzadas, etc.

Ver todas tus listas ()

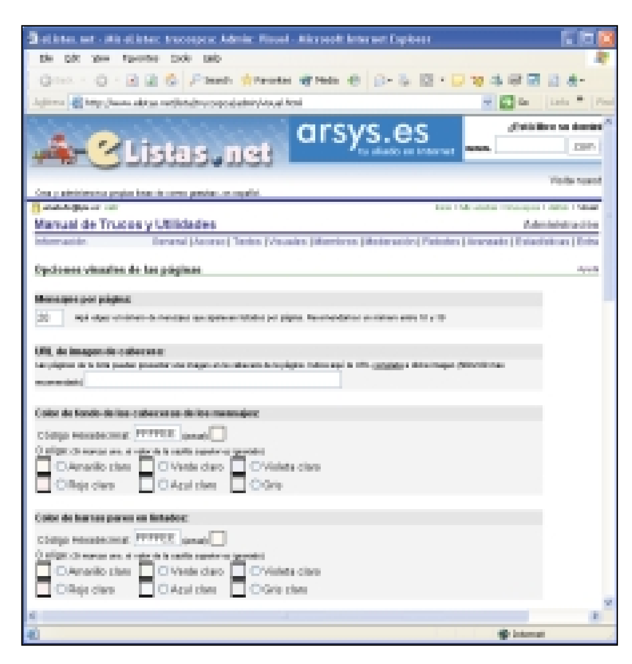
Desde la página *Mis eListas* tendremos acceso directo a todas nuestras listas en eListas.net, así como a las que estemos suscritos.

Dar a conocer esta lista (*www.eListas.net/lista/[nombre_de_la_lista]/admin/promo.html*)

En esta página encontraremos el código HTML necesario para poder promocionar nuestra lista en páginas web, crear casillas de suscripción en nuestras páginas, etc. Simplemente tendremos que elegir el tipo de formulario de inscripción que queremos e incrustar el código en nuestro editor de páginas web.

Paso 11
Administrar nuestra lista

La configuración general de nuestra lista de correo (dirección, nombre de la lista, URL de la página sobre la lista, palabras clave, breve descripción y categoría), pueden ser modificadas desde la dirección *lista]/admin/general.html*. En la página *www.eListas.net/-lista/[nombre_de_la_lista]/admin/acceso.html*, podremos ver los valores de acceso a la lista definidos durante la creación de la misma y que podremos modificar: si puede suscribirse cualquiera o necesita la confirmación del administrador, quién podrá

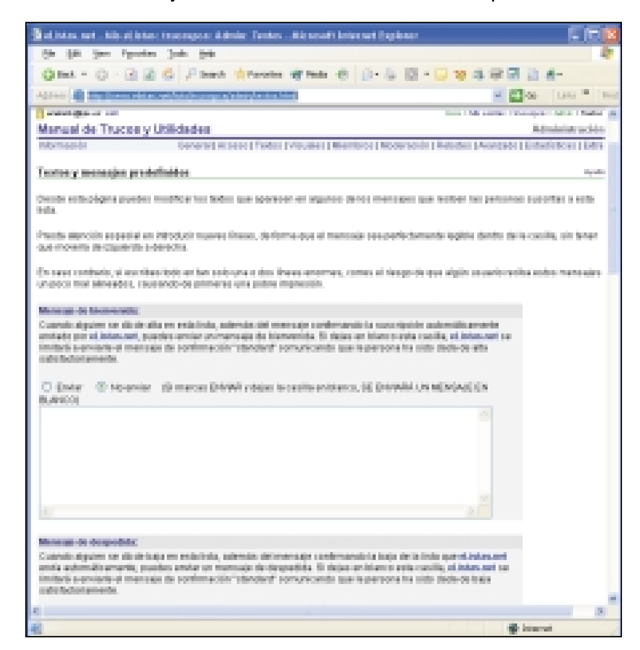


enviar mensajes a la lista de correo, si la lista de correo será moderada, quiénes tendrán acceso a los mensajes archivados, páginas web de la lista, la base de datos, el área de ficheros, o el área de encuestas, así como la difusión de la lista (pública o privada). Las estadísticas de altas y bajas de usuarios las encontraremos en la página, mientras que la configuración de las opciones visuales de las páginas web de administración de la lista de correo podremos encontrarla en *www.eListas.net/lista/[nombre_de_la_lista]/admin/visual.html*

Paso 12
Textos y mensajes predefinidos

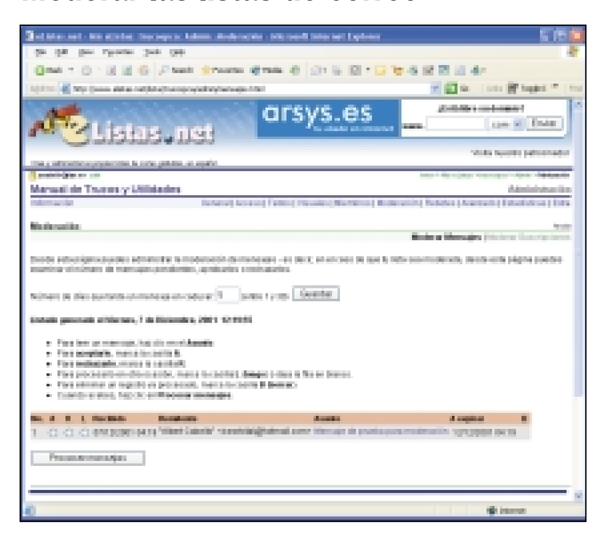
Desde la página *www.eListas.net/lista/[nombre_de_la_lista]/admin/textos.html*, en cualquier momento, podremos programar nuestros mensajes predefinidos. Estos mensajes son:

Bienvenida: será enviado cuando alguien se dé de alta en nuestra lista junto con la confirmación de suscripción. Básica-



mente incluirá la presentación de la lista y su propósito, así como las normas de uso de la misma.
Mensaje de despedida: este mensaje será enviado cuando alguien se dé de baja en nuestra lista, junto con la confirmación de baja.
Firma en mensajes: lo que añadamos en esta casilla se añadirá al final de todos los mensajes enviados a través de la lista de correo. Debe contener un máximo de 4 o 6 líneas con información de utilidad para los usuarios de la lista.
Firma en mensajes HTML: si utilizamos código HTML en nuestros mensajes de la lista de correo, podremos definir una firma HTML, de manera que nos sea posible incluir gráficos, *banners* o hiperenlaces a páginas web de interés para los usuarios de la lista.
Etiqueta en el asunto: si queremos que el asunto de los mensajes de correo enviados a la lista empiecen por una etiqueta que ayude a identificar dichos mensajes, la incluiremos bajo esta casilla. Por defecto, el contenido de esta etiqueta será [nombre_de_la_lista]
Auto-responders predefinidos: aquí introduciremos el contenido de los archivos de información y preguntas más frecuentes, que serán enviados cuando un usuario mande un correo electrónico a las direcciones *[nombre_de_la_lista]-info@eListas.net* y *[nombre_de_la_lista]-faq@eListas.net*, respectivamente.

Paso 13
Moderar las listas de correo



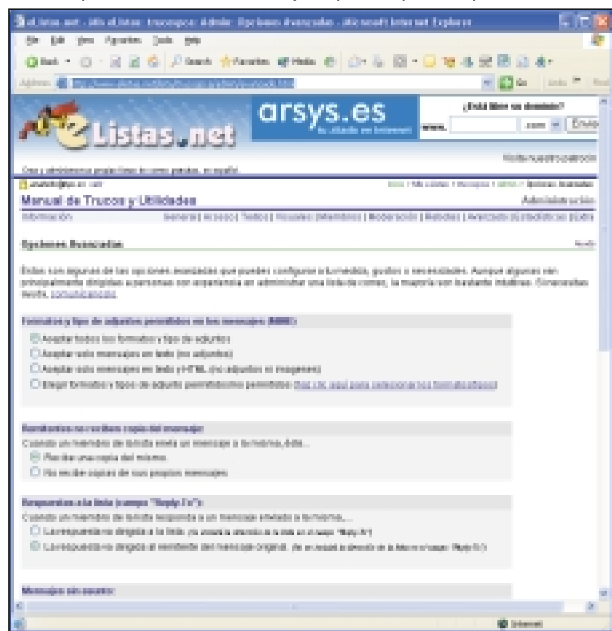
Si hemos definido nuestra lista de correo como moderada, todos lo mensajes que sean enviados a ella serán almacenados temporalmente hasta que el moderador decida qué hacer con ellos: enviarlos, eliminarlos o simplemente responder al emisor. Desde la página *www.eListas.net/lista/[nombre_de_la_lista]/-admin/mensajes.html* podremos administrar la moderación de mensajes, es decir, podremos examinar el número de mensajes pendientes y decidir si aprobar su envío o rechazarlo, así como el número de días que tardará un mensaje en caducar si no es revisado y, por ende, desechado. En la ventana veremos una lista con los mensajes que tenemos pendientes por moderar. Para leer un mensaje haremos clic sobre el asunto; para aceptarlo, marcaremos la casilla «A»; para rechazarlo, la casilla «R»; y para moderarlo más adelante, la casilla «L» (de «Luego»). Para eliminar un registro ya procesado, marcaremos la casilla «B» (de «Borrar») y, cuando terminemos, haremos clic sobre el botón *Procesar mensajes*. Estas mismas opciones las tendremos desde el mensaje que también habrá sido enviado a la cuenta de correo del administrador de la lista.

Configuración de preferencias de usuarios

En la página web *www.eListas.net* encontraremos una serie de enlaces o apartados que nos facilitarán la configuración de la lista de correo a la que estamos suscritos según nuestras preferencias. Echemos un vistazo.
Para ver las listas a las que estamos suscritos: *www.eListas.net/misListas*
Para revisar y modificar las preferencias de usuario: *www.eListas.net/lista/[nombre_de_la_lista]/misprefs.html*
Para consultar mensajes atrasados:
www.eListas.net/lista/[nombre_de_la_lista]/archivo
Para enviar un mensaje: *www.eListas.net/lista/[nombre_de_la_lista]/enviar*
Para mantener bases de datos como agendas, enlaces a páginas y FAQ:
www.eListas.net/lista/[nombre_de_la_lista]/datos
Para descargar o subir ficheros:
www.eListas.net/lista/[nombre_de_la_lista]/ficheros
Para crear o responder encuestas:
www.eListas.net/lista/[nombre_de_la_lista]/encuestas
Para consultar o notificar eventos:
www.eListas.net/lista/[nombre_de_la_lista]/eventos

Paso 14
Opciones avanzadas

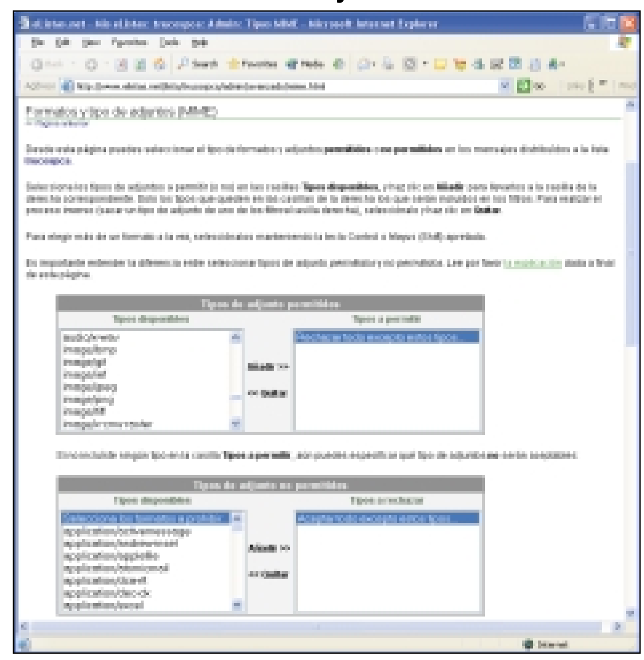
En la página de opciones avanzadas (*www.eListas.net/lista/-[nombre_de_la_lista]/admin/avanzado.html*), podremos configurar algunas de las opciones avanzadas de nuestra lista de correo, que están dirigidas especialmente a personas con niveles de experiencia en la administración de listas. Estas opciones son las siguientes.
Remitentes no reciben copia del mensaje: aquí definiremos si un miembro de la lista podrá o no recibir, como usuario, una copia de su mensaje cuando envíe un mensaje a la lista.
Respuestas a la lista (campo «Reply-To»): cuando un miembro de la lista responda a un mensaje enviado a la misma, la respuesta podrá ir dirigida a la lista. (incluyéndose la dirección de la lista en el campo «Reply-To») o al remitente del mensaje original (no se incluirá la dirección de la lista en el campo «Reply-To»).
Mensajes sin asunto: opción que se definirá para que la lista pueda aceptar o no mensajes con el asunto en blanco.
Aceptar o rechazar mensajes que empiecen por «suscribe»,



etc…: a veces, la gente enviará a la lista mensajes con comandos como «subscribe», «unsubscribe», etc. Desde aquí especificaremos si se aceptarán o se desecharán automáticamente estos mensajes.
Tamaño mínimo y máximo de los mensajes: aquí definiremos el tamaño mínimo y máximo (en caracteres) que estará permitido para los mensajes enviados a la lista.
Responder a usuarios en la lista negra: cuando un usuario en la lista negra envíe un mensaje a alguna de las direcciones de correo de nuestra lista (*[nombre_de_la_lista]@eListas.net* o *[nombre_de_la_lista]-comando@eListas.net*,...) especificaremos si le informaremos de que no se le permite enviar mensajes a nuestra lista o si simplemente ignoraremos el mensaje, sin enviar respuesta alguna a dicho usuario.

Paso 15

Filtrado de archivos adjuntos

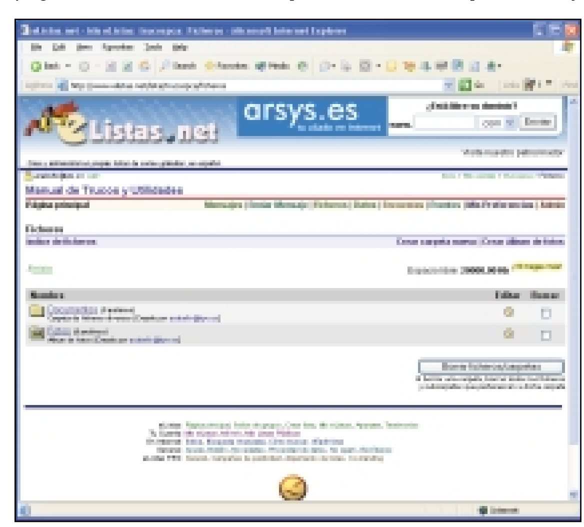


En la página *www.eListas.net/lista/[nombre_de_la_lista]-/admin/avanzado.html* seleccionaremos las reglas para los *Formatos y tipos de adjuntos permitidos en los mensajes (MIME)*. Las opciones disponibles son *Aceptar todos los formatos y tipos de adjuntos*, *Aceptar sólo mensajes de texto (sin adjuntos)*, *Aceptar sólo mensajes de texto y HTML (sin adjuntos ni imágenes)* y *Elegir formatos y tipos de adjuntos permitidos/no permitidos*. Si seleccionamos esta última opción accederemos a la página *www.eListas.net/lista/[nombre_de_la_lista]/admin/avanzado/mime.html* donde podremos seleccionar el tipo de archivos adjuntos permitidos y bloqueados en los mensajes distribuidos a través de la lista de correo. En esta página encontraremos dos apartados: *Tipos de adjunto permitidos* y *Tipos de adjunto no permitidos* con una amplia lista de formatos de archivos que podremos seleccionar y añadir o quitar de cada una de ellas. Cuando seleccionemos uno o más formatos *permitidos*, eListas eliminará de los mensajes cualquier tipo de formato que no coincida con los especificados bajo la casilla *Tipos a permitir*. Dejando esta casilla en blanco, el filtro aceptará todos los formatos y tipos, pasando a procesar el filtro de *Tipos de adjunto no permitidos*. En este caso, eListas procesará el mensaje revisando que los archivos adjuntos incluidos no coincidan con alguno de los tipos incluidos bajo la casilla *Tipos a rechazar*.

Paso 16

Cómo compartir ficheros

Como toda comunidad de usuarios que se precie, nuestra lista de correo dispondrá de un espacio donde todos los usuarios podrán compartir ficheros. Este espacio se encuentra en la página *www.eListas.net/lista/[nombre_de_la_lista]/ficheros* y

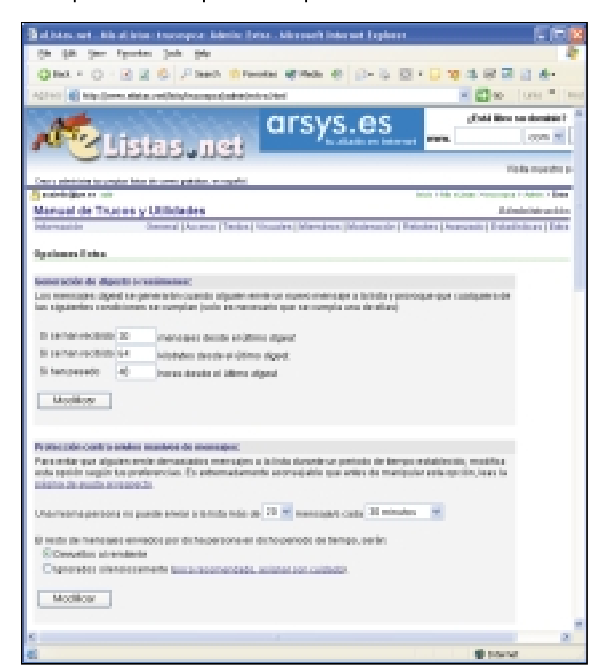


ofrece 20 Mbytes de capacidad. Allí los administradores podrán crear o eliminar carpetas o álbumes de fotos y todos los usuarios podrán descargar los ficheros que el administrador haya decidido compartir.

Paso 17

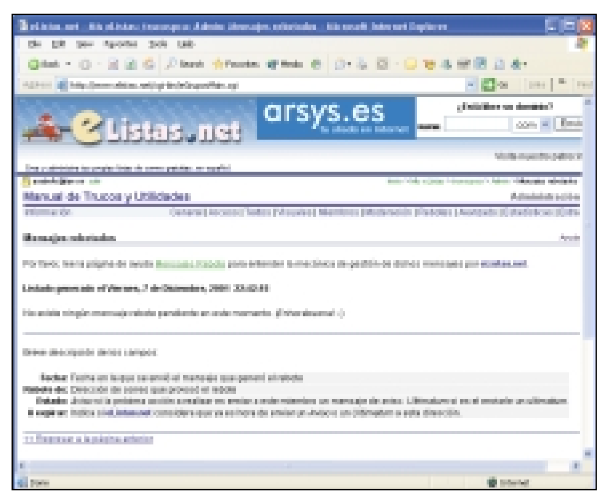
Reducir el número de mensajes y combatir el *spam*

Las listas de correo son bastante interactivas. Cuando mandemos un mensaje a una lista, el servidor lo distribuirá inmediatamente a todos los suscriptores y podremos esperar que algunos de ellos respondan el mensaje, iniciando una discusión que de rebote pueda colapsar nuestro buzón de entrada



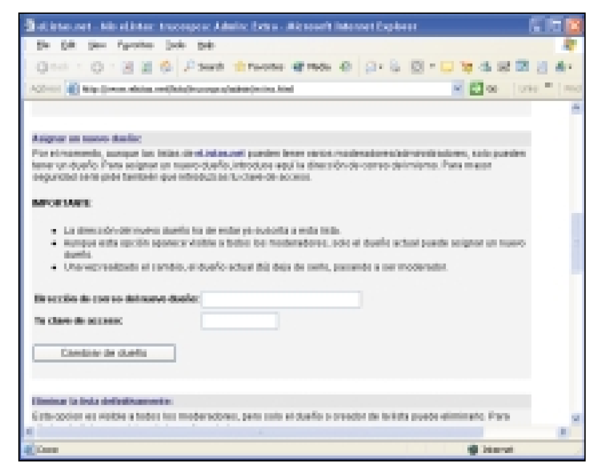
de correo electrónico y también acabar con nuestra paciencia. De la misma forma, en algunos casos puede ser molesto porque no queramos ser interrumpidos mientras estamos, por ejemplo, en el trabajo, o no queramos recibir gran cantidad de mensajes relacionados con el mismo tema, y prefiramos leer todos estos mensajes en nuestros ratos libres de una forma ordenada y rápida. Para ello, en la página *www.eListas.net/-lista/[nombre_de_la_lista]/admin/extra.html,* seleccionaremos los parámetros de *Digest* para nuestra lista de correo, definiendo por número de mensajes, número de Kbytes o número de horas que transcurrirán entre cada uno de los *digests*. De esta forma, podremos definir si solamente queremos recibir un mensaje diario conteniendo toda la conversación hecha durante esas últimas 24 horas al fin del día. Estos resúmenes no serán editados, de forma que recibiremos exactamente la misma información que si estuviéramos suscritos en la modalidad habitual pero agrupándose dentro de un único mensaje. Bajo este mismo apartado encontramos la herramienta de protección contra el envío masivo de mensajes, que podremos definir de forma que no sean aceptados un número superior de mensajes de un mismo remitente en un periodo de tiempo establecido, así como también si estos mensajes serán devueltos al remitente o ignorados sin notificación alguna al remitente.

Paso 18
Mensajes rebote



Un mensaje rebote en una lista de correo se asemeja a cuando nos devuelven una carta convencional porque no pudo entregarse a su destinatario. Normalmente, si un mensaje enviado desde nuestra lista de correo no consigue llegar al destinatario, siempre se generará un mensaje rebote desde el servidor que gestiona ese buzón de correo para informar al remitente que nuestro mensaje no llegó a buen puerto. Cuando se tiene una lista de muchos miembros, especialmente si la lista es abierta y se suscribe quien quiere, es inevitable que se generen mensajes rebote, incluso si todas las direcciones de correo en la lista son correctas y pertenecen a personas reales, ya que estos errores pueden ser debidos a que, por ejemplo, la cuenta del usuario se encuentre llena. Sea cual sea la causa por la que se genere un mensaje rebote, eListas tomará nota del usuario y del mensaje rebotado, y guardará esta información en una cola especial de correo, archivando el mensaje rebote para que el administrador supervise su contenido, y enviará automáticamente un aviso al usuario. En el caso de que este mensaje no rebote, eListas intentará enviar el mensaje original de nuevo, y si rebota, volverá a tomar nota y guardará otra vez la información en la cola especial de correo, repitiendo este aviso a los 7-12 días. Si a los 7-12 días de enviar el segundo mensaje de aviso, estos vuelven a rebotar, eListas mandará un mensaje de ultimátum al usuario y en el caso de que éste también rebote, el servidor de la lista asumirá que la cuenta no está operativa y dará al usuario de baja. En la página *www.eListas.net/lista/[nombre_de_la_lista]/admin/-rebotes.html* podremos comprobar y administrar el número de mensajes rebote que se hayan dado en nuestra lista.

Paso 19
Cambiar el dueño de la lista



Como ya sabéis, la lista de correo es administrada en el aspecto técnico por un dueño que además de definir el carácter y las reglas de la lista, como por ejemplo el tema de la lista, y cuáles son las reglas generales que todos los inscritos deben aceptar para tomar parte en ella, también actúa como árbitro (única función que podrá delegar en otros usuarios llamados moderadores). El dueño de la lista es responsable de todos los asuntos administrativos y de contestar preguntas de los inscritos a la lista. No es raro tener varios moderadores compartiendo la responsabilidad entre ellos, en particular en listas «técnicas», donde un moderador con experiencia técnica ayude a otro. Para cambiar el dueño de una lista, en la página *www.eListas.net/lista/[nombre_de_la_lista]/admin/extra.html* nos desplazaremos hasta el campo *Asignar un nuevo dueño* e introduciremos la dirección de correo electrónico del nuevo dueño junto con nuestra clave de acceso para verificar el cambio realizado.

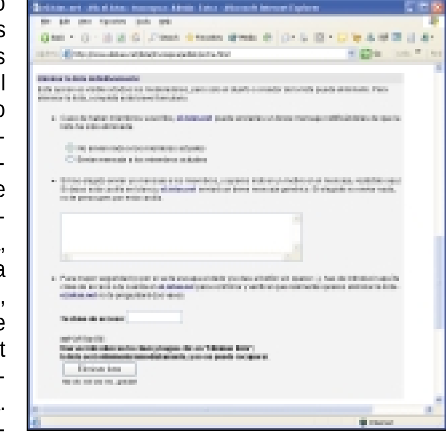
Cambios a los parámetros de la lista

Si estamos pensando hacer cambios en los parámetros de configuración de nuestra lista, como norma general informaremos de estos cambios al grupo. Si, por ejemplo, cambiamos el modo de lista de pública a privada, o de moderada a no moderada, será necesario advertir previamente a las personas que utilizan la lista, y explicarles las razones del cambio de parámetros y cómo afectará a la lista. Es importante que consultemos al grupo antes de tomar este tipo de decisiones. A menudo, el grupo mismo impulsará algunos de estos cambios como respuesta a sucesos relacionados con la lista.

Paso 20

Eliminar la lista definitivamente

Esta opción, visible a todos los moderadores, pero sólo operativa por el dueño creador de la lista, se encuentra dentro de la página *www.eListas.net/lista/[nombre_de_la_lista]/admin/extra.html*. Para eliminar la lista completaremos el formulario existente. En caso de tener miembros suscritos, podremos enviar un mensaje notificando el cese del servicio que proporcionaba la lista. Si hemos elegido enviar un mensaje a los miembros, podremos indicar el motivo en el mensaje, redactándolo en el cuadro disponible para el efecto. Si dejamos esta casilla en blanco, se enviará un breve mensaje genérico generado automáticamente. Si optamos por no enviar nada, no hay que preocuparse por esta casilla. Para mayor seguridad, deberemos introducir nuestra clave de acceso a la cuenta en eListas.net para confirmar y verificar que realmente queremos eliminar la lista. Hay que tener en cuenta que eListas.net no nos preguntará dos veces para confirmar la eliminación. Una vez introducida nuestra clave y después de hacer clic en el botón *Eliminar lista*, la lista será eliminada inmediatamente y no se podrá recuperar.

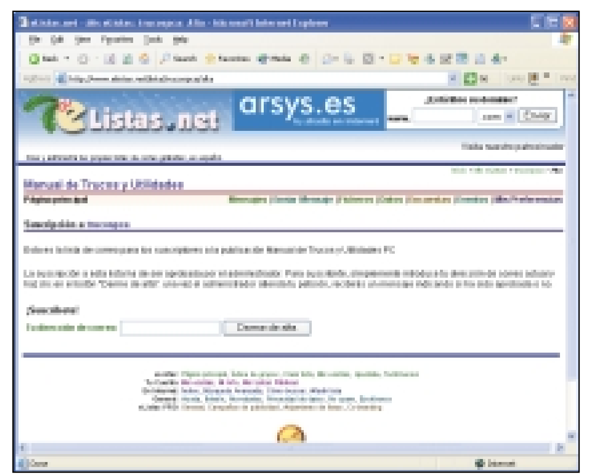


Acceder y participar en una lista de correo

Paso 21

Alta y baja en una lista de correo

Para recibir y enviar mensajes a una lista de correo será necesario darse previamente de alta mandando un mensaje en blanco a la dirección de suscripción de la lista (*[nombre_de_la_lista]-alta@eListas.net*) o a través de la página web *www.eListas.net/-lista/[nombre_de_la_lista]/alta*. En ese momento recibiremos un mensaje de correo electrónico con el que confirmaremos el alta en la lista de correo seleccionada, bien respondiendo al mensaje o accediendo al enlace web incluido en el mensaje. Una vez confirmada la suscripción recibiremos una clave que verificará nuestra cuenta de acceso y que podremos utilizar para definir nuestras preferencias de configuración, y comenzaremos a recibir los correos de otros miembros de la lista. Para enviar un mensaje al resto de usuarios, simplemente enviaremos un correo electrónico a la dirección correspondiente a esa lista *[nombre_de_la_lista]@eListas.net*. Si queremos contestar un mensaje y que la respuesta llegue a todos los miembros del foro usaremos la opción *Responder a todos* en nuestro programa de correo. Si vamos a responder únicamente a la persona que envió el mensaje utilizaremos la opción *Responder*. En cada lista de correo será bienvenido cualquiera que quiera hablar sobre los temas propuestos, y muy probablemente serán expulsados aquellos que manden mensajes fuera de tema, agresivos o publicitarios y que no tengan que ver con la lista de correo, o que no cumpla las normas de esa lista.



Para darnos de baja de una lista de correo mandaremos un mensaje en blanco a la dirección *[nombre_de_la_lista]-baja@eListas.net* o introduciremos nuestra cuenta de correo electrónico en la página *www.eListas.net/lista/[nombre_de_la_lista]/baja*.

Paso 22

Otros servicios de listas de correo

Coollist (*www.coollist.com*): Servidor que ofrece listas de correo o discusión gratuitas. Permite agregar los e-mail de los miembros automáticamente. Puede ser moderada o no.

Yahoo! Groups (*http://groups.yahoo.com*): Muy fácil de administrar. Admite listas moderadas y no moderadas, pero también se pueden crear listas en las que sólo el administrador puede enviar mensajes, que pueden servir para comunicar actualizaciones de páginas web, nuevos productos, etc. Permite adjuntar archivos a los mensajes, incluso si éstos ocupan 100 Kbytes. Tiene un sistema que evita el *spam*, de forma que sólo los inscritos pueden enviar mensajes y sólo desde el buzón con el que se suscribieron.

Delphi: Muy sencillo de contratar y configurar. Las listas pueden ser de carácter público o privado, así que si sólo queremos crear una lista con nuestros familiares y que nadie se entere de lo que están hablando, aquí lo podremos hacer. También ofrece servicio de chat.

Group Mail (*www.group-mail.com*): Controla tu propio sistema de lista de correo con este programa.

Hyperlist (*www.hiperlist.com*): Otro sitio en español donde alojar una lista de correo gratuita que nos puede servir tanto para comunicarnos con nuestros amigos como para mantener un grupo de discusión sobre un tema particular, o bien, si tenemos una empresa, comunicarnos con todos nuestros clientes enviando boletines sobre nuestros nuevos productos.

Internet Soccer Fans Association: Permite crear una lista de correo gratuita únicamente si su temática está relacionada con el fútbol.

ListApp (*http://server.com/WebApps*): Servidor de listas de correo. Ofrece varios servicios para tu página, como libro de visita, agenda, etc.

Mi correo (*http://micorreo.org/ListasCorreo*): Servicio básico de listas de correo en el que la única persona que podrá enviar mensajes a los miembros de una lista será el administrador de la misma. Por lo que para lo único que podemos utilizar este servicio es para enviar comunicados, distribuir alguna revista electrónica o bien, si tenemos una empresa, distribuir comunicados entre los clientes. Sitio en español.

PostMaster General (*www.es.postmastergeneral.com*): Servicio gratuito para listas de correo de hasta 30 destinatarios. Depura automáticamente direcciones electrónicas incorrectas, permite exportar e importar archivos, programar mensajes, crear la interfaz para inscripción de direcciones electrónicas y otras características de integración con el sitio web.

Topica (*www.topica.com*): Servidor gratuito para listas de correo. Podemos crear listas de discusión, moderadas o no, y tipo *newsletter*, e incluso *digest*.

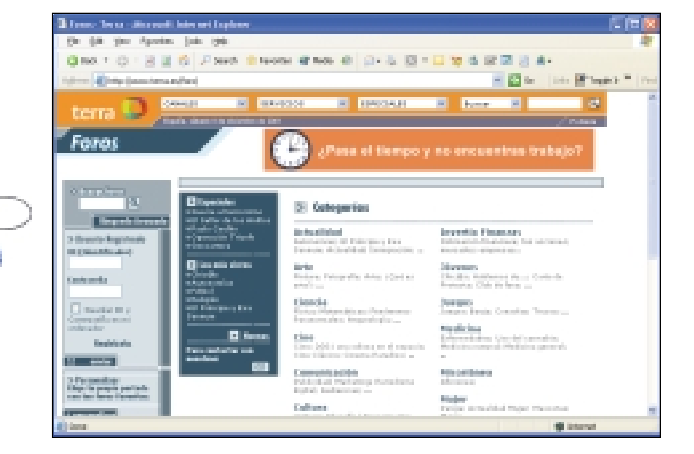


Foros web de discusión

Cómo funciona este lugar de encuentro de internautas

Intermedio

Los foros web de discusión imitan a los tradicionales grupos de noticias, con lo que consiguen dotar de interactividad a las páginas web en las que se encuentren. Es una opción interesante para todo tipo de páginas; sus usuarios podrán entrar y debatir sin necesidad de estar conectados simultáneamente. Cualquier persona con acceso a Internet puede, a través de su navegador web, acceder a leer las opiniones de los internautas en estos foros. Los foros de discusión son el lugar de encuentro donde los usuarios pueden resolver sus dudas y dar solución a problemas de otras personas, consultar determinados asuntos, aportar ideas y trucos o simplemente hablar de temas de interés común. En el siguiente artículo queremos dar una imagen general del funcionamiento de los foros de discusión, ya que todas las características aquí expresadas no son comunes a todos los foros.



Estructura y funcionamiento

Paso 1

Estructura de los foros

La organización de los foros depende en gran medida del tipo de contenidos del foro y de la visión del administrador que los haya creado. Existen tres tipos de foros, de los que podremos encontrar todos o sólo algunos de ellos en cualquier página web:

Foros Generales: son aquellos donde se tratan temas de interés general, de aspectos relacionados con las secciones del sitio web. Normalmente, cualquier usuario puede acceder a ellos para leer o enviar mensajes.

Foros Privados: para acceder a estos es necesario conocer su clave de acceso, que es determinada por el administrador de los foros. Este es el responsable de facilitar la clave a los usuarios que él quiera que participen en su foro.

Foros Personales: son los foros creados por los propios usuarios. De esta forma, los usuarios tienen un lugar para que se hable de los temas que más les interesen.

A su vez, estos foros se componen de grupos donde se clasifican los diferentes temas de discusión y que servirán para orientar inicialmente a la participación, aunque los foros de discusión están abiertos para tratar otros temas que los participantes puedan aportar. Estos grupos se componen de *topics* y *subtopics*, que son cada una de las discusiones iniciadas por algún usuario. Entre los diferentes grupos, podemos encontrar:

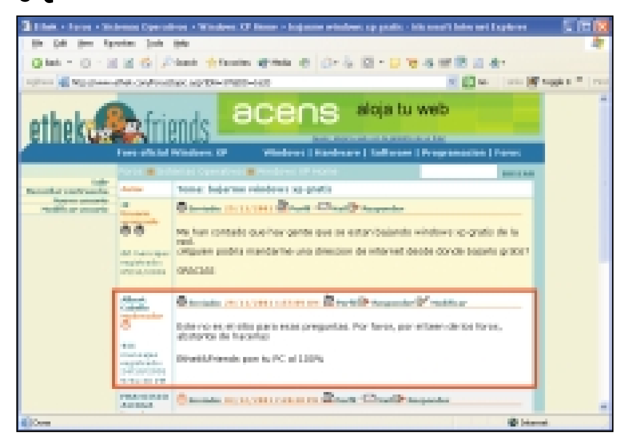
Anuncios: el administrador puede crear un grupo donde únicamente los administradores y moderadores puedan enviar y publicar mensajes. Este tipo de grupos suele ser utilizado como grupos de anuncios, es decir, mensajes enviados por el moderador del foro o el administrador que no pueden ser respondidos por ningún usuario. Si deseamos opinar sobre algún anuncio específico, tendremos que crear un nuevo tema en el foro apropiado.

Archivo: el foro puede contener un área de archivo, lugar de acceso de sólo lectura que contendrá temas que anteriormente estuvieron en los foros. No podremos contestar los temas que se encuentran archivados. Los temas archivados pueden eliminarse por completo de su foro original o bien pueden quedar en el mismo sin que sea necesario eliminarlos.

Temas activos del día: a través de esta opción podremos ver todos los mensajes, en los foros públicos, que hayan sido enviados durante el día en curso.

Paso 2

¿Quiénes son los moderadores?

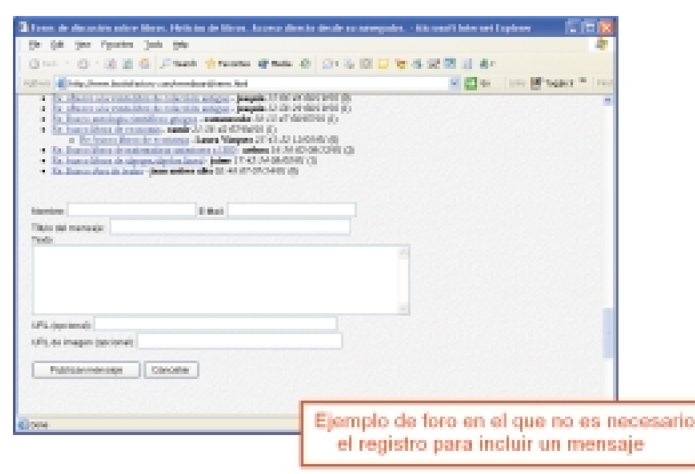


Los moderadores controlan individualmente los foros. La figura del moderador es la garantía para los usuarios de que serán tratados con el respeto que merecen. Por ello, es a él a quien deben dirigirse las posibles quejas o preguntas sobre el contenido de los mensajes ya publicados o el funcionamiento del foro en cuestión. Un moderador es quien reconduce el debate siempre que lo considere necesario. Para ello tiene la capacidad de editar, borrar o recortar cualquier texto o imagen enviados en sus foros. Por ello, en ocasiones los administradores de los foros censurarán ciertas palabras que puedan encontrarse en el contenido de un mensaje. Se trata de una censura que no es muy exacta y real, ya que en ocasiones ésta se basa en el contexto de las palabras y se realiza de forma automática mediante unos *scripts*: por ejemplo, las palabras que deban ser censuradas en cierto foro se cambiarán por asteriscos (*).

Paso 3

¿Necesito registrarme?

Dependiendo de cómo el administrador haya configurado los foros podremos participar libremente de forma anónima o únicamente podremos ver los mensajes pero no contestarlos. Es posible saber si los envíos anónimos están permitidos si podemos enviar un mensaje sin necesidad de completar los campos *Nombre de usuario* y *Contraseña* cuando se nos pregunte o si ni siquiera existen estos campos. Sin embargo, normalmente el registro es necesario para aquellas personas que desean enviar o contestar mensajes. Para participar es necesario que primero se rellene el formulario con los datos requeridos. El registro suele ser gratuito y no estamos obligados a enviar mensajes con nuestro nombre real, de forma que podemos utilizar apodos. De cualquier manera, es necesario que introduzcamos una dirección de correo electrónico real, ya que normalmente se recibirá un mail de confirmación para poder finalizar la configuración del acceso al foro en cuestión. Esta dirección de correo electrónico sólo será utilizada en el caso de que nos olvidemos de la contraseña, y normalmente tenemos la opción de esconder nuestra dirección de correo de los ojos del resto de usuarios, a excepción del administrador. Para crear una cuenta de usuario, habitualmente pulsaremos sobre el botón *Nuevo usuario* o *Edit Profile*, si bien en algunos casos será necesario contactar directamente con los moderadores del foro para que nos proporcionen acceso. En este caso, nos aseguraremos de incluir nuestro nombre real completo, dirección de correo electrónico y nombre de usuario o apodo preferido.



Ejemplo de foro en el que no es necesario el registro para incluir un mensaje

Paso 4

Beneficios de estar registrado

Si un foro distingue entre usuarios registrados y no registrados, normalmente los usuarios registrados contarán con ciertos privilegios frente a los anónimos. Estos son:

-Posibilidad de incluir nuestro nombre completo y la dirección de correo electrónico en nuestros envíos.

-La ventaja de recibir notificaciones por mail cuando alguien responda algunos de los envíos que hayamos seleccionado como de nuestro interés.

-Posibilidad de cambiar nuestra propia contraseña.

-En algunos foros, la facilidad de especificar otras preferencias que afectan a la utilización del foro, y ofrecer mayor información sobre nosotros al resto de usuarios.

-Crear foros, tener un apodo reservado, utilizar emoticonos en los mensajes, etc.

Paso 5

Extravío del nombre de usuario y/o clave de acceso

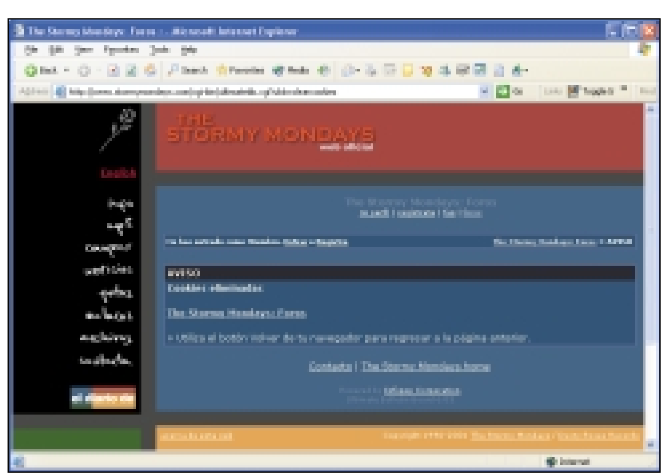
Si hemos olvidado el nombre de usuario y/o la clave de acceso para unos foros en los que es necesario el registro, podremos recuperarlos pulsando sobre el botón *Recordar contrase-*



ña (*Forgotten your password*) que encontraremos normalmente en la página principal de los foros o en la página de composición de un nuevo mensaje. Este enlace nos llevará a una página donde introduciremos los datos que verifiquen nuestra identidad, que en ocasiones se limitarán a nuestro *nick* o nuestra dirección de correo electrónico. El sistema nos enviará nuestra clave o una nueva generada de forma aleatoria a la dirección de correo electrónico asociada a nuestro registro, para recobrar así el acceso a los foros.

Paso 6
Cookies

La mayoría de foros utilizan *cookies* para almacenar la información sobre el usuario: la última vez que visitó el foro, el nombre de usuario, la clave de acceso, la cantidad de mensajes mostrados, la identificación única cada vez que se inicia sesión; en definitiva, el método empleado por el programa para reconocer las «preferencias de usuario», aquellas que se hayan elegido durante la configuración del acceso a los foros o en una sesión anterior. Estas *cookies* suelen ser grabadas en la memoria del navegador. No se utilizan para ver cuál es el uso que se hace de los foros, pero si se opta por desactivar el soporte de las *cookies* o el navegador las bloquea o no incluye soporte, algunas de las opciones que permitirán ahorrar tiempo no funcionarán adecuadamente. Si tenemos problemas para iniciar sesión dentro de los foros, podrá ser debido a un conflicto con alguna de las *cookies* que se encuentren en nuestro navegador. En este caso, algunos foros de mensajes tienen un enlace que



tratará de limpiar todas las *cookies* relacionadas con el foro de mensajes. Lo encontraremos en la dirección *www.servidor.com/-cgi-bin/ultimatebb.cgi?ubb=clearcookies*

Participar en los foros

Paso 7
Añadir un mensaje

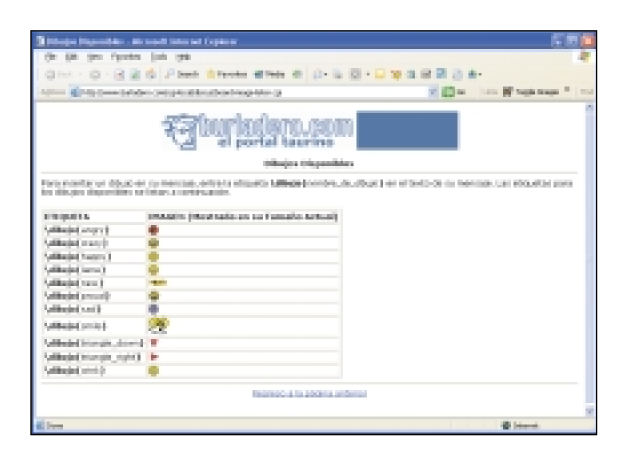
Para añadir un mensaje a una discusión existente, pulsaremos sobre el botón *Añadir respuesta* o *Post a reply* que se encontrará normalmente en la parte superior o inferior de la página cuando visualicemos una discusión. Dependiendo de la configuración de los foros, podremos dar formato a nuestros mensajes utilizando un código especial o en ocasiones haciendo



uso de *tags* HTML. Si lo que queremos es crear una nueva conversación para comenzar una nueva discusión, pulsaremos sobre el botón *Nuevo mensaje* o *Add a new message*. Esto añadirá un *Subtópico* con el asunto que hayamos especificado, con lo que comenzaremos una nueva conversación en la que el mensaje inicial será el que hemos especificado. Tras rellenar la línea *Asunto*, seguiremos las instrucciones mencionadas anteriormente para enviar nuestro mensaje.

Paso 8
Cómo usar emoticonos

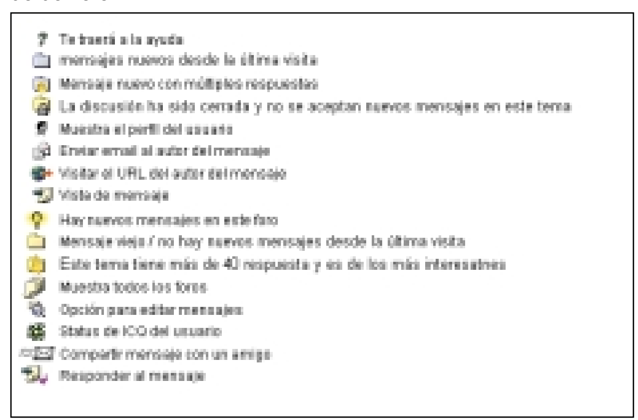
Los emoticonos son pequeñas imágenes que expresan estados de ánimo, y al igual que los utilizamos en chats o conversaciones de correo electrónico podremos también decorar nuestros mensajes en los foros web. En la gran mayoría de foros podremos asociar un icono con cada uno de los mensajes enviados, cada uno de los cuales expresará una emoción diferente. Estos iconos aparecerán al lado de cada mensaje en el listado de temas de cada foro. Adicionalmente, también



podemos insertar emoticonos en el contenido de nuestro mensaje. Para ello, tendremos que insertar junto con el texto del mensaje los códigos de los que queremos que aparezcan, que serán unos u otros dependiendo de los foros a los que accedamos. Incluso en algunos casos, los mismos foros transformarán automáticamente algunos *smileys* clásicos como :), :(a su representación gráfica. Por ejemplo si escribimos :o en un mensaje, automáticamente se convertirá en una cara vergonzosa o sorprendida. Otros foros utilizan la siguiente simbología: \dibujo{*nombre_de_dibujo*}

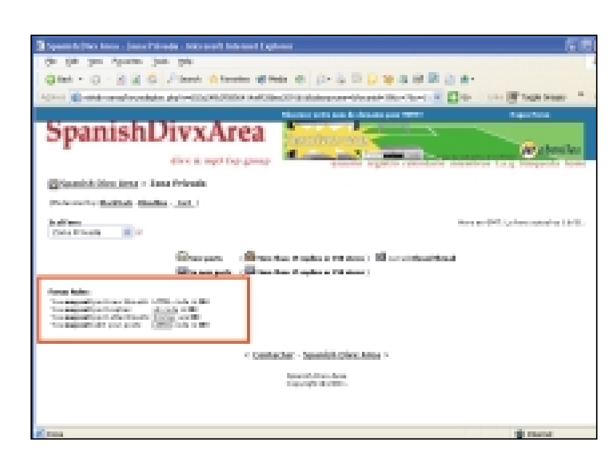
Paso 9
Otros iconos

Además de los iconos que incluimos en nuestros mensajes, los mismos foros web de discusión pueden asignar iconos a los *Topics* o *Asuntos* de las conversaciones. Entre ellos destacan los siguientes, aunque pueden ser diferentes dependiendo del foro.



Paso 10
Uso de HTML y/o código BB

Una gran cantidad de foros web de discusión utilizan código HTML y/o código BB, si bien los administradores o moderadores puede desactivar su uso, en cuyo caso el *script* únicamente mostraría los *tags* de código pero no serían ejecutados. Estos códigos pueden ser utilizados en el cuerpo del mensaje y en el asunto del mismo. El código BB es una variación de los clásicos *tags* HMTL con los que muchos estaremos ya familiarizados. Básicamente, este código nos permite añadir funcionalidades o estilos a nuestros mensajes que normalmente requerirían una gran cantidad de código HTML. Podemos utilizar el código BB incluso si HTML no está activado en el foro en el que lo estemos utilizando, con la ventaja añadida de que se requiere menos código y su uso es más seguro (una sintaxis o codificación incorrecta no acarrearía tantos problemas como cuando se utiliza HTML).



Paso 11
Tags de código BB

Para darnos la posibilidad de que decoremos nuestros mensajes con textos en negrita, en cursiva, diferentes colores y tamaños de letras ponemos a vuestra disposición una serie de etiquetas que podremos incluir en los mensajes y que posteriormente serán convertidas automáticamente en etiquetas HTML. Los **tags** de código BB más usuales son:

-**Hiperenlaces URL**

Si el código BB esta activado en un foro, no necesitaremos utilizar el **tag** [URL] para crear un hipervínculo. Simplemente escribiremos la URL completa y el hiperenlace será creado automáticamente

http://www.yourURL.com

www.yourURL.com

Observaremos que podemos utilizar la dirección completa con *http://* o acortarla comenzando con el dominio *www*. Si el sitio no comienza con *www*, deberemos introducir la dirección completa comenzando por *http://*. También serán automáticamente creados los enlaces que comiencen por los prefijos *https* o *ftp*.

Sin embargo, podemos utilizar el Viejo código [URL] encasillando el hiperenlace tal y como está detallado a continuación (el código BB está en negrita): **[url]**www.vnunet.es**[/url]**

También podremos crear hiperenlaces al estilo de los existentes en páginas web si utilizamos el siguiente formato: **[url=http://www.vnunet.es]**Web de vnunet**[/url]**

En los ejemplos anteriores, el código BB automáticamente generará un hiperenlace a la URL que se encuentre encasillada. Esto asegurará que el enlace será abierto en una nueva ventana cuando el usuario haga clic sobre él. En el segundo ejemplo, el texto especificado hará de hiperenlace a la URL introducida.

-**Enlaces a direcciones de correo electrónico**

Para añadir un enlace a una dirección de correo electrónico en nuestro mensaje, únicamente encerraremos la dirección de correo electrónico tal y como se muestra en el siguiente ejemplo (el código BB está en negrita):

[email]acabello@bpe.es**[/email]**

En el ejemplo anterior, el código BB generará automáticamente un enlace a la dirección de correo electrónico especificada.

-**Negrita y cursiva**

Podemos poner en cursiva o negrita el texto, si encerramos las secciones de nuestro texto con los *tags*

[b] [/b] (para negrita) o [i] [/i] (para cursiva Hola , [b]Alberto[/b] Hola, [i]Olivia[/i]

-**Añadir imágenes**

Para añadir un gráfico dentro de nuestro mensaje, únicamente encerraremos la URL de la imagen siguiendo el siguiente ejemplo (donde el código BB está en negrita):

[img]http://www.vnunet.es/imagenes/logo.gif**[/img]**

En el ejemplo anterior, el código BB automáticamente transforma la imagen en visible dentro del mensaje. Conviene recordar que la parte *http://* de la orden es necesaria para el correcto funcionamiento del código [img]

-**Citar otros mensajes**

Para hacer referencia a una parte específica de un mensaje que otro usuario haya enviado, simplemente copiaremos y pegaremos el texto a referenciar, encerrándolo según el siguiente ejemplo (el código BB está en negrita):

[QUOTE]No dejes para mañana...
lo que puedas hacer pasado mañana.**[/QUOTE]**

En el jemplo anterior, el código BB automáticamente generará un índice que hará referencia al texto que hemos indicado.

-**Code Tag**

Similar al *tag* utilizado para citar contenidos de otros mensajes, el *tag* de código sirve para preservar el formato de un texto, útil para mostrar por ejemplo código de programación de un programa:

[CODE] !/usr/bin/perl
print «Content-type: text/html\n\n»;
print «¡Hola Mundo!»; **[/CODE]**

En el ejemplo anterior, el código BB automáticamente bloquea todo el texto al que se hace referencia y mantiene el formato del texto encerrado.

Paso 12

Uso incorrecto del código BB

No debemos utilizar código HTML y código BB para realizar la misma función. Además, observaremos que el código BB no es sensible a la capitalización de letras, de forma que [URL] y [url] son la misma orden:

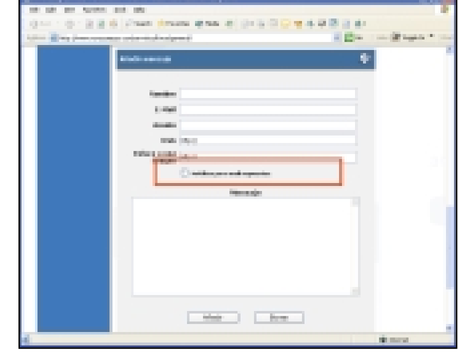
[url] www.vnunet.es [/url] – No debemos poner espacios entre el código entre corchetes y el texto al que queremos aplicar el código.

[email]acabello@bpe.es[email] – El corchete final debe incluir una barra invertida ([/email])

Paso 13

Adjuntar archivos y notificaciones por mail al responder nuestro mensaje

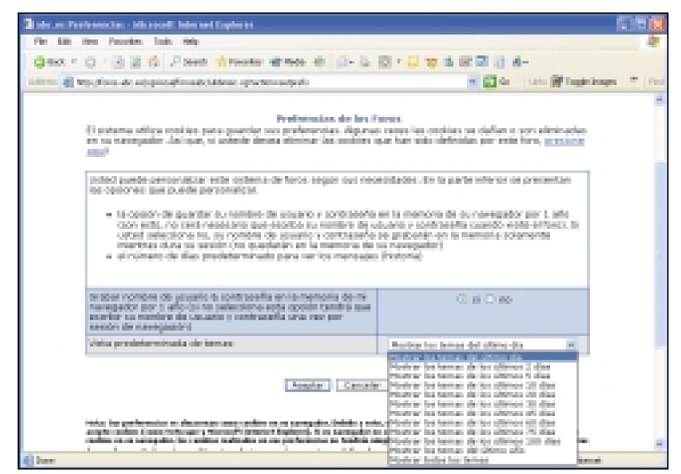
Por razones de seguridad, no podremos enviar archivos adjuntos con nuestros mensajes. Sin embargo, sí podremos copiar y pegar texto de cualquier documento en nuestro mensaje, o utilizar código HTML y/o código UBB (si su uso está habilitado por el administrador) incluyendo un hipervínculo a una dirección URL que contenga ese archivo. Para concluir, al enviar un nuevo mensaje a un foro de discusión, en la ventana de composición del mensaje tendremos la opción de definir si deseamos ser notificados en la dirección de correo electrónico asociada a nuestra cuenta de usuario cuando alguien responda nuestro mensaje. Esta opción resulta especialmente útil en foros de discusión en los que nuestro grado de participación es muy alto y podamos perder la vista a una conversación, o especialmente en aquellas conversaciones en las que tengamos gran interés. Únicamente marcaremos en la ventana de composición del mensaje la casilla de *Notificación por Correo Electrónico*, si deseamos utilizar esta opción.



Paso 14

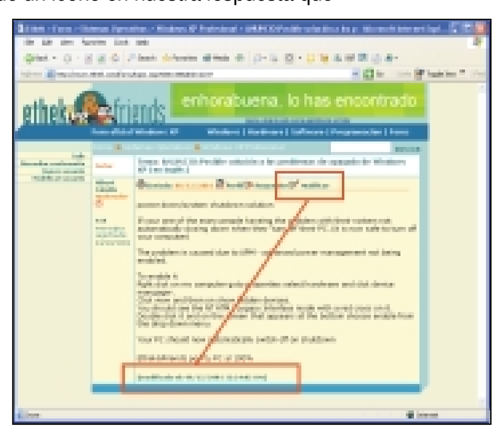
Personalizar el aspecto de los foros y nuestro perfil de usuario

De una manera sencilla, y siempre dependiendo de la configuración que el administrador haya decidido para los foros, podremos modificar en mayor o menor medida la información contenida en nuestro perfil de registro, utilizando el botón *Perfil* localizado en la parte superior de cada página. En la nueva página aparecerá toda la información de nuestro perfil. Como usuario registrado, podremos cambiar muchos aspectos, a excepción expresa de nuestro *Nombre de Usuario*. Por ejemplo, podremos dejar grabado en nuestro navegador el nombre de usuario y contraseña durante un periodo máximo de un año, para no tener que autenticarnos manualmente cada vez que entremos en los foros. Si queremos cambiar la dirección de correo electrónico, y el administrador del foro tiene activado la verificación de correo electrónico, automáticamente se nos asignará una nueva contraseña a nuestra nueva dirección de correo electrónico. En algunos casos, podremos personalizar la apariencia de los mismos en nuestro navegador, seleccionando alguna de las opciones que el administrador nos haya proporcionado. Además, si el administrador lo permite, quizás tengamos la opción de crear nuevos temas visuales para los foros. Al crear un nuevo tema, podremos seleccionar colores, fuentes y tamaños de fuente utilizados en el foro, si bien únicamente el administrador podrá cambiar las imágenes para cada tema, de forma que cuando un usuario cree un tema, serán utilizadas las imágenes por defecto del foro. Además, tendremos la opción de personalizar la cantidad de días de los que nos mostrará temas y/o mensajes enviados en los diferentes foros. En ocasiones también podremos introducir la zona horaria en la que nos encontramos, de modo que todos los horarios de los mensajes en los foros de discusión aparezcan en nuestro horario local. Por ejemplo, si estamos en una zona horaria 5 horas menor que donde se encuentra el foro, introduciremos «-5». Los cambios realizados serán actualizados inmediatamente en la base de datos.



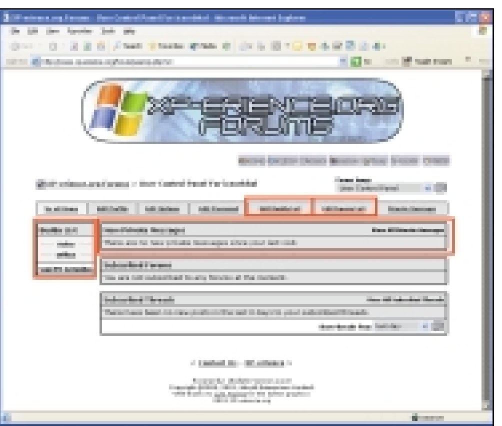
Paso 15
Editar nuestros propios mensajes

Si el foro de discusión lo permite, podremos editar nuestros propios mensajes cualquier día y a cualquier hora. Para ello, iremos al hilo de discusión donde enviamos nuestro mensaje y comprobaremos la existencia de un icono en nuestra respuesta que nos permita su edición. Nadie más a excepción de nosotros, y del moderador y/o el administrador de los foros podrá editar nuestro mensaje. Al hacerlo, se generará una nota haciendo mención de que el mensaje ha sido editado, de forma que toda la gente que lea el mensaje sepa quién y cuándo modificó su contenido. Además, durante los 30 minutos siguientes en los que enviamos un mensaje, la ventana de edición del mensaje nos dará la opción de eliminar ese mensaje. Transcurrido ese tiempo, únicamente el moderador y/o el administrador podrán eliminar un mensaje. Tendremos en cuenta que si nuestro mensaje era el comienzo de un nuevo hilo de discusión, eliminar este mensaje tendrá como consecuencia la eliminación de la conversación por completo, y todas las respuestas serán también suprimidas. A su vez, el administrador del foro puede deshabilitar la posibilidad de que los miembros editen o eliminen sus mensajes. Para editar o eliminar mensajes, será necesario ser un usuario registrado de los foros.



Paso 16
Mensajes privados

Los administradores de un foro web de discusión pueden permitir a sus miembros enviarse mensajes privados unos a otros. Un mensaje privado entre miembros en un foro de discusión no es un correo electrónico. Los mensajes privados son comunicaciones «uno-a-uno» que únicamente pueden ser leídas por el destinatario. Podremos leer estos mensajes a través de una sección que encontraremos en la página de nuestro perfil de usuario. Dentro de la configuración de nuestro perfil, estableceremos si queremos que se nos notifique a través del correo electrónico cuando alguien intente enviarnos un mensaje privado así como también es posible evitar que nos envíen mensajes privados configurando la opción apropiada. Únicamente los miembros registrados podrán enviar mensajes privados. La gestión de los mensajes privados se realiza a través de dos carpetas:



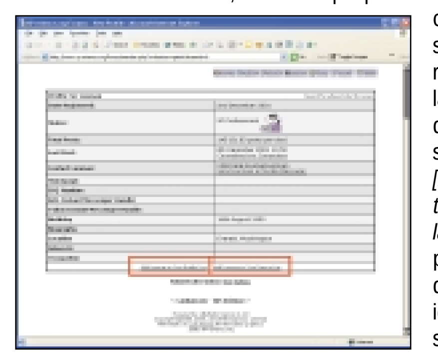
-La *Bandeja de entrada*: contendrá todos los mensajes que nos hayan sido enviados. Podremos leerlos o eliminarlos desde allí.

-La *Bandeja de salida o elementos enviados*: en ella se almacenarán todos los menajes que hemos enviado a otros usuarios, como recordatorio de los mensajes que hemos enviado y a quién. También podremos leer o eliminar los mensajes desde aquí.

Si queremos enviar un mensaje privado a otro usuario, buscaremos el botón de *Mensaje privado* en un mensaje creado por la persona con la que queremos contactar. También podremos enviar un mensaje privado a través del perfil de miembro, o a través de nuestra lista de contactos, si hemos añadido esa persona a dicha lista. Introduciremos un título para el mensaje, y si los emoticonos están permitidos en el foro, también podremos utilizarlos.

Paso 17
Listas de contactos y de usuarios ignorados

Tanto las listas de contactos como la de usuarios ignorados afectan únicamente a los mensajes privados. Las listas de contactos permiten reunir, en una única ubicación centralizada dentro de nuestro perfil, todos nuestros contactos dentro de los foros, de forma que podamos enviar de una forma rápida y sencilla un mensaje privado a esa persona. Es posible introducir un usuario en nuestra lista de contactos o a la lista de usuarios ignorados accediendo al perfil de ese usuario y pulsando sobre los enlaces *Añadir [nombre_usuario] a la lista de contactos* o *Añadir [nombre_usaurio]a la lista de usuarios ignorados* respectivamente. Cualquier usuario que se encuentre en nuestra lista de ignorados no podrá enviarnos mensajes privados.

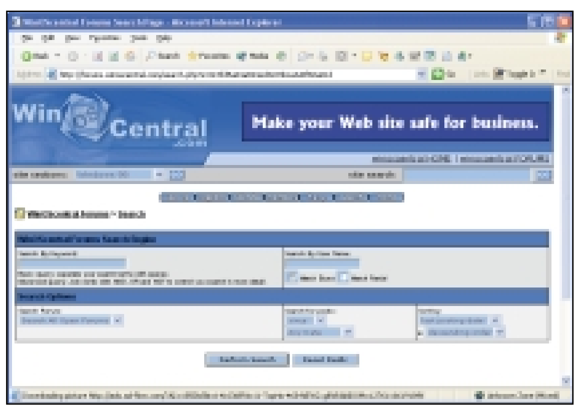


Paso 18
Búsquedas de mensajes específicos

Podemos localizar mensajes específicos de nuestro interés en los foros efectuando búsquedas que estarán basadas en el momento de envío de los mensajes (búsqueda de «Nuevos mensajes») o por concordancia de textos (búsqueda «por palabras clave»). Cada uno de estos métodos de búsqueda dispondrá de los mecanismos adecuados para localizar las discusiones de nuestro interés.

En el primero de los casos, para buscar nuevos mensajes, iniciaremos si es necesario sesión con nuestro nombre de usuario y contraseña en las casillas apropiadas y buscaremos los mensajes desde nuestra última visita a los foros o desde la fecha que especifiquemos. En cualquier caso, podremos buscar nuevos mensajes haciendo uso de una de las opciones restantes. Por ejemplo, las opciones «ayer» y «semana pasada» serán equivalentes a buscar los mensajes emitidos el día anterior o la semana anterior, respectivamente.

Para realizar una búsqueda en el foro basándonos en una palabra o un conjunto de ellas, pulsaremos dentro del cuadro *Búsqueda por palabras* para especificar la palabra o palabras que utilizaremos en la búsqueda. Las instrucciones adicionales se mostrarán en la misma pantalla de búsqueda, en la que podremos restringir la búsqueda de esas palabras clave dentro del cuerpo de los mensajes, asuntos, nombres de autores, fecha, etc., así como también limitar la búsqueda a algún foro en particular.

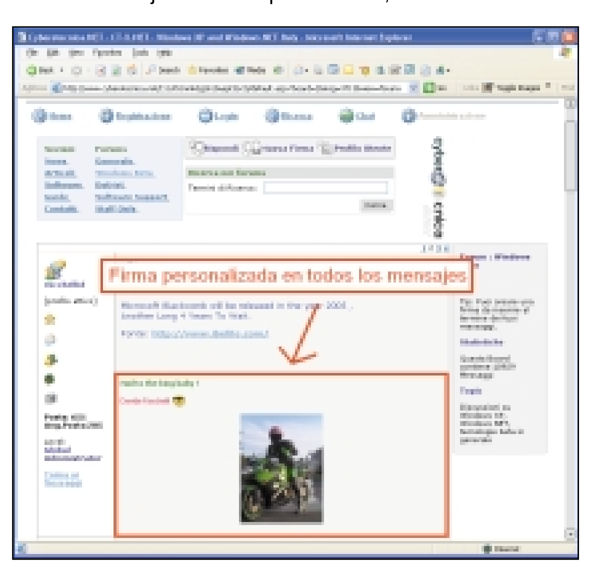


Cuando hayamos realizado dicha búsqueda, pulsaremos sobre cualquiera de los enlaces propuestos para abrir las páginas que contengan las conversaciones seleccionadas. Cuando el foro de discusión cuente con grupos privados, únicamente podremos realizar búsquedas en los grupos particulares para los que tengamos acceso, y sólo los administradores y moderadores podrán realizar búsquedas en todos los grupos. Para buscar en los foros privados, necesitaremos validar nuestra identidad de usuario con nuestro nombre y contraseña. Conviene tener en cuenta que los mensajes en el grupo de *Anuncios* no se incluirán dentro de los resultados de la búsqueda.

Paso 19

Uso de firmas

Dependiendo del funcionamiento y objetivo del foro, tendremos la posibilidad de utilizar firmas personalizadas en nuestros mensajes en los foros de discusión de la misma forma que mucha gente las utiliza en sus mensajes de correo electrónico. Esta opción de firma personalizada puede activarse y ser modificada pulsando sobre el enlace *Perfil* que encontraremos en la parte superior de la mayoría de las páginas. Esta firma se incluirá en la parte inferior de cada mensaje, y en ocasiones estará limitada a un tamaño de tres líneas. Una vez tengamos la firma grabada en nuestro perfil, podremos incluirla en todos mensajes que enviemos marcando la opción *Incluir firma cuando escribamos un mensaje* o de forma individual marcando la opción que se nos presentará en la página de composición de mensajes. De cualquier manera, el administrador de los foros puede decidir desactivar las firmas personalizadas en cualquier momento. Si este es el caso, la opción para incluir nuestra firma personalizada no nos aparecerá cuando enviemos un mensaje, aunque tengamos grabada nuestra firma en el perfil. Hay que tener en cuenta que siempre que el administrador haya habilitado estas opciones, podremos utilizar *tags* HTML o código BB (excepto el código BB para imágenes) para nuestras firmas.



Paso 20

Niveles de usuario

Algunos foros tienen establecidos unos métodos para clasificar a los usuarios por su actividad en los mismos, es decir, por el número de mensajes enviados. A modo de ejemplo, incluimos los niveles de usuario de los foros del sitio web Maxreboot.com, en *www.maxreboot.com/forums*

Tipo de usuario	Nº mínimo de envíos	Nº máximo de envíos
«Usuario Suspender»	0	9
«Usuario Cerrar Sesión»	10	29
«Usuario Reiniciar»	30	49
«Usuario Apagar Sistema»	50	99
«Usuario Hard Boot»	100	199
«Usuario BSOD»	200	499
«Necesito un nuevo hobby»	500	899
«De camino a los mil»	900	999
«¡Hola! Mi nombre es...y soy un adicto a los foros de MaxReboot»	1.000	1.100
«¡¡El Dios de los foros!!»	1.101	2.000
«De vuelta al manicomio voy... »	2.001	3.000

El administrador tiene la opción de asignar un nivel diferente al usuario que escoja. Así mismo, los administradores de un foro web de discusión pueden permitir a los miembros clasificarse unos a otros. Únicamente los usuarios registrados pueden ser clasificados y a su vez sólo pueden ser clasificados por otros usuarios. Incluso si las clasificaciones se utilizan en un foro de discusión concreto, podemos seleccionar en nuestro perfil una opción que no permita que seamos clasificados pro el resto de miembros. Esta opción también podrá ser deshabilitada por los administradores de los foros de discusión.

Paso 21

Reglas y «Netiquette»

Los foros de discusión son un espacio en el que se debe debatir con libertad sobre cualquier tema que deseemos. Es normal que entre usuarios en ocasiones haya desacuerdos totales en opiniones, ideas y hechos, pero el debate siempre debe mantener el respeto hacia las otras personas. Por ello, los administradores se reservan el derecho a eliminar aquellas opiniones y vetar el acceso a los foros a los usuarios que:

-Promuevan actividades ilegales (pornografía infantil, terrorismo, etc.).

-Difundan de manera ilícita información o programas protegidos por las leyes internacionales de Copyright.

-Inciten a la violencia.

-Faciliten información personal sobre algún internauta sin su consentimiento.

-Contengan insultos o empleen un lenguaje obsceno o blasfemo de forma sistemática, o cualquier otra expresión que descalifique a personas, colectivos o instituciones (recordamos que escribir en mayúsculas en Internet equivale a gritar).

-Contengan mensajes publicitarios.



Control remoto de equipos

Manejar a distancia un PC

Intermedio /

Las posibilidades de controlar una máquina de forma remota hace muchos años que ya existe. Desde los primeros tiempos de Unix y su variante Linux, existen comandos que permiten administrar y controlar una máquina de manera remota a través de una red o una conexión telefónica. Sin embargo, es relativamente reciente el control remoto mediante interfaz completamente gráfica. El omnipresente Windows es el último protagonista de esta historia. Ahora bien, antes de comenzar a explicar las distintas posibilidades que existen a la hora de control remoto, hemos de entender qué podemos hacer exactamente.

En primer lugar, conviene tener en cuenta que, en cualquiera de los casos que vamos a comentar a continuación, vamos a tener ante nosotros un auténtico *Escritorio* de Windows dentro de una ventana que se ejecuta en nuestra máquina. Esto significa que nuestro teclado y ratón serán los encargados de simular que nos encontramos delante del PC al que nos conectamos, y que todo lo que ejecutemos, borremos, carguemos o hagamos se hará en la máquina remota, nunca en nuestro PC. Por esta razón, hemos de tener mucho cuidado, puesto que no tendremos acceso físico al ordenador remoto. Un apagado accidental, por ejemplo, nos obligará a que alguien pulse de nuevo la corriente para seguir trabajando.

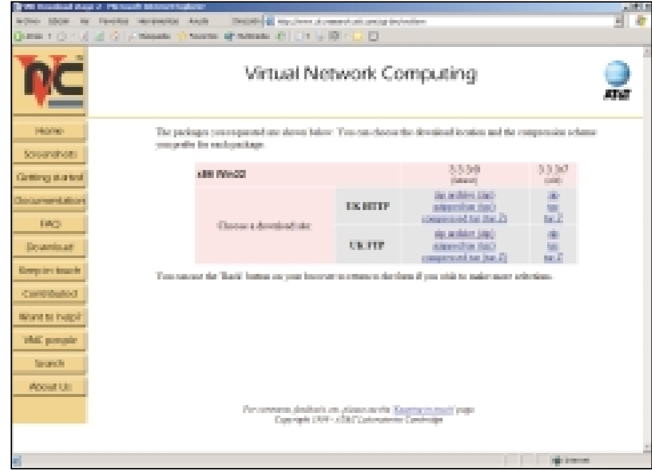
Pero hablemos un poco más de las utilidades. Entendemos que existen dos casos bien diferenciados. El primero es que necesitemos acceder a la máquina para operar con ella, desde consultar datos, hasta trabajar con sus aplicaciones o documentos. El segundo es que, sobre todo en el caso de los servidores, nos conectemos a ella con el objeto de administrar su funcionamiento y verificar que todo marcha correctamente. No hace falta que imaginemos el ahorro de tiempo y la comodidad que supone para un administrador de sistemas controlar los servidores desde su propia casa mientras está enfermo o de vacaciones, sin necesidad de desplazarse. Lo mismo podríamos decir de un usuario que tenga, por ejemplo, necesidad de acceder a la aplicación que sólo un compañero posee en un ordenador en toda la oficina. Este método le evitará tener que levantarse para consultar el dato en pantalla.

Ahora bien, a continuación vamos a distinguir entre dos posibilidades muy bien diferenciadas. La primera será la conexión de dos PC mediante un programa *freeware*, más concretamente el VNC. Su sencillez de funcionamiento y coste cero lo convierten en un candidato ideal para necesidades sencillas. La segunda y tercera opción que trataremos será la característica de *Acceso Remoto* que Windows 2000 Server y Windows XP Profesional incluyen de serie y que nos permitirán realizar estas tareas de un modo mucho más avanzado, aunque fundamentalmente se orientarán a administrar un servidor o ejecutar alguna aplicación de elevados requerimientos que sólo puede ejecutarse en él.

VNC

Paso 1
Descargar software

Lo primero que tendremos que hacer es descargar la última versión del VNC (siglas de *Virtual Network Computing*) desde la dirección *www.uk.research.att.com/vnc*. Aquí acudiremos al área de descarga (pinchar sobre *Download* en la barra de botones de la izquierda), y decidiremos qué paquete de todos los disponibles descargaremos. En nuestro caso, dado que vamos a trabajar sobre plataformas Windows, nos haremos con la versión *x86*. Sin embargo, tal y como podréis ver en la página, tenemos disponible la versión de esta misma aplicación para Linux, Unix, Sun o Mac, entre otras plataformas.



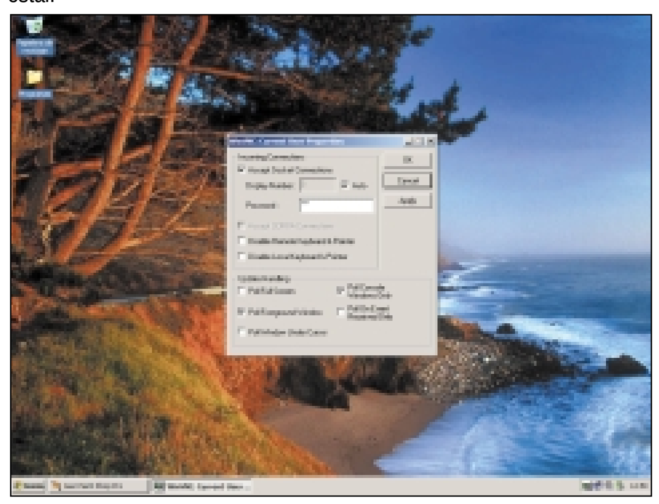
Una vez descargado en nuestro ordenador, no tendremos más que descomprimir el fichero «.zip» y proceder a instalar la aplicación utilizando el habitual archivo «setup.exe». Ahora bien,

este proceso sólo será necesario llevarlo a cabo con el equipo al cual deseamos acceder, ya que el PC desde el que nos conectemos no precisará más que ejecutemos el programa «vncviewer.exe» que se adjunta dentro del mismo fichero «.zip».

Paso 2

Poner a punto el *host*

Una vez instalado VNC en la máquina que hará de *host*, es decir, el equipo al cual nos vamos a conectar de forma remota, sólo tendremos que acudir al menú de *Inicio/Programas/VNC* y hacer clic sobre *Run WinVNC (App Mode)*. La primera vez que ejecutemos esta aplicación tendremos en pantalla una ventana en la que nos solicitará que fijemos las opciones de funcionamiento. Lo primero que debemos hacer es fijar una contraseña en la casilla *Password*, ya que es imprescindible para que el programa funcione. En caso de que no estemos interesados en ella, podemos poner un solo número o letra, aunque en cualquier caso, ha de estar.

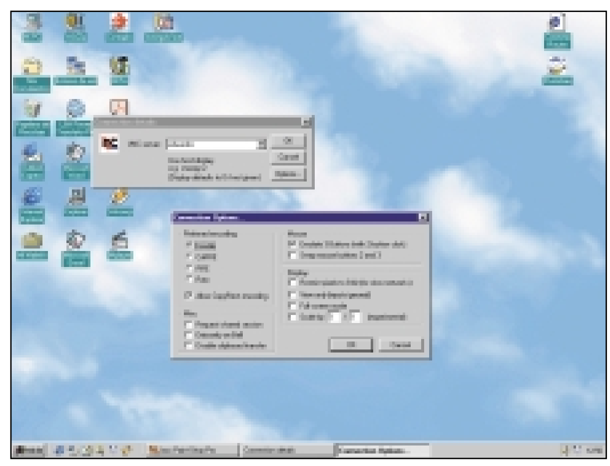


Además, podremos hacer que cuando se conecten a esta máquina se desactiven el ratón y teclado del ordenador remoto (con *Disable Remote Keyboard&Pointer*) o los de esta máquina (con *Disable Local Keyboard&Pointer*). Por último, tendremos algunas opciones adicionales, como la utilización de pantalla completa (*Poll Full Screen*).
Una vez hayamos terminado de ajustar los parámetros de esta ventana, no tendremos más que pulsar *Ok*, y veremos que aparece un nuevo icono en la *Barra de tareas*, junto al reloj. Ahora este PC está listo para recibir las conexiones entrantes desde otros PCs. Como es lógico, damos por hecho que para que esto sea posible, este PC está conectado a una red que funciona bajo protocolo TCP/IP y que se encuentra perfectamente configurada.

Paso 3

En el equipo cliente

Ahora será el momento de probar que la conexión funciona correctamente. Como dijimos en el primer paso, sólo será necesario que nos hagamos con el fichero «vncviewer.exe» que se encuentra en el ZIP que descargamos de Internet. Dado que ocupa 172 Kbytes, no tendremos mayores problemas para meterlo en un disquete o pasarlo por red a la/s máquina/s que necesitemos. Una vez en la máquina cliente, desde la que nos conectaremos al *host*, no tendremos más

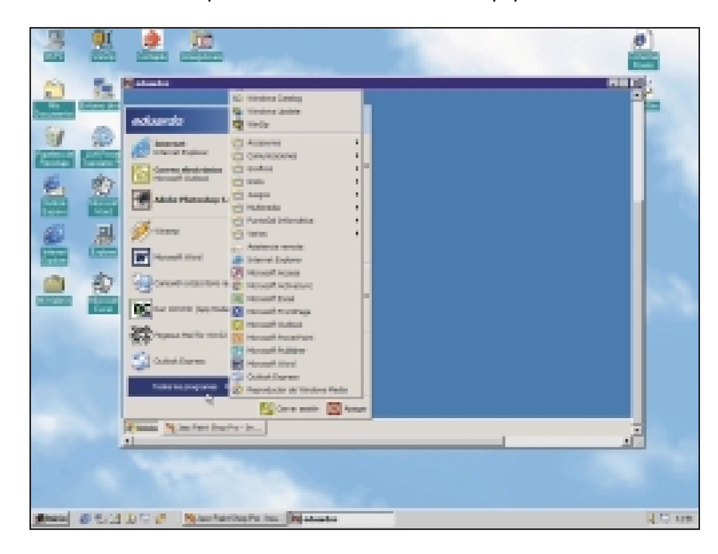


que ejecutar este archivo haciendo doble clic sobre él. Ante nosotros se abrirá una pequeña ventana en la que hemos de indicar el nombre exacto que tiene en la red el equipo al que nos queremos conectar o, alternativamente, su dirección IP si la conocemos.

Paso 4

Posibles configuraciones

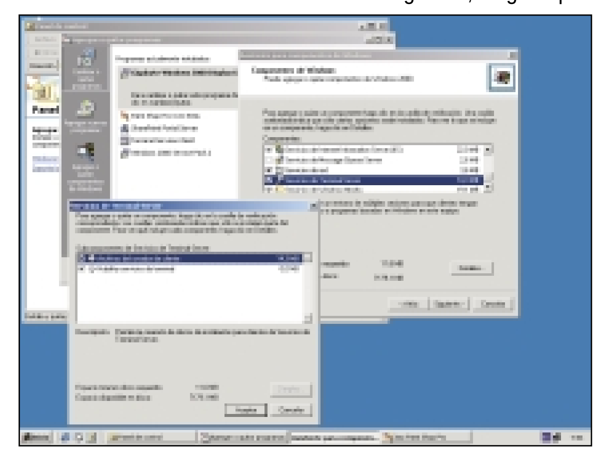
Ahora bien, si pinchamos sobre *Options*, veremos que es posible ajustar algunos parámetros, tales como la emulación de los tres botones del ratón o el intercambio de los botones 2 y 3 de este mismo dispositivo. Muy interesante resulta la opción *Restrict pixels to 8-bit*, que bajará la calidad de la imagen del escritorio del otro equipo y, por tanto, la cantidad de imagen transmitida por la red. En redes muy congestionadas o con problemas de ancho de banda, esta opción nos resultará muy útil. Igual de importante es *Full-screen mode*, con la que se mostrará el escritorio de la otra máquina a pantalla completa. No olvidemos que, para salir de este modo, tendremos que pulsar la tecla de *Inicio* del teclado o «Ctrl + Esc». Después, haremos clic con el botón derecho sobre el icono de Vncviewer de la barra inferior y *Close*.
Por último, cuando terminemos con estos parámetros, pulsaremos *Ok*, y en la ventana de conexión que antes teníamos, volveremos a pulsar *Ok*. Si el nombre es correcto, la red funciona y ajustamos correctamente el equipo *host*, se nos pedirá la contraseña de acceso. Tras introducirla, tendremos en nuestra pantalla el escritorio del otro equipo.



Terminal Server en Windows 2000

Paso 1
Primeros pasos

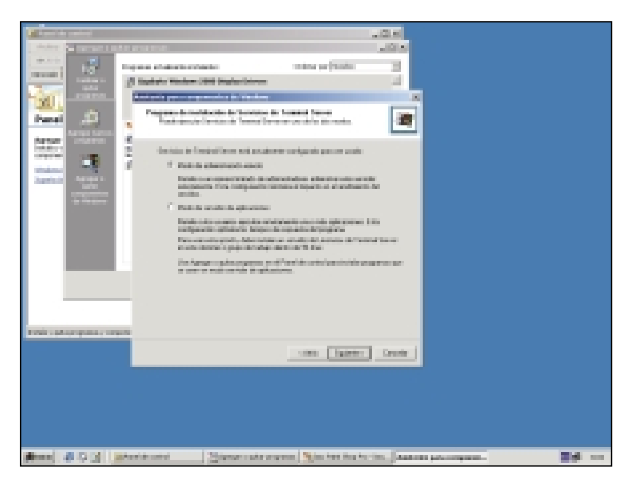
Antes de empezar a pensar en utilizar los servicios de Terminal Server en Windows 2000 Server, tendremos que realizar algunas pequeñas comprobaciones en el equipo que hará de servidor. De nuevo, daremos por hecho que este equipo cuenta con la interfaz de red correctamente configurada, al igual que



el resto de los equipos desde los que deseamos acceder a él. Lo primero será acudir a *Inicio/Configuración/Panel de Control*, donde seleccionaremos *Agregar o quitar programas*. En la nueva ventana pincharemos sobre *Agregar o quitar componentes de Windows*, tras unos momentos de espera, aparecerá ante nosotros una completa lista de componentes que podremos instalar o desinstalar, y que hacen referencia al propio sistema operativo. La que nos interesa especialmente es una de las que se sitúa hacia el final de la lista, concretamente *Servicios de Terminal Server*. Hemos de comprobar si está o no instalada y, además, pinchando en *Detalles*, verificaremos que incluye la opción *Archivos del creador de cliente*. Hayamos o no tenido que pinchar sobre alguna de estas opciones, pulsaremos el botón *Siguiente* de esta ventana, ya que con ello comenzaremos el proceso de configuración.

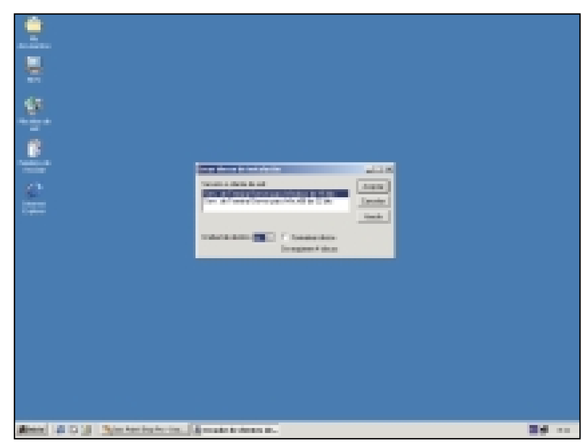
Paso 2
Configurar el servicio

Después de lo anterior, lo primero que tendremos que ajustar será la pantalla en la que decidiremos sobre el modo en que utilizaremos los servicios de Terminal Server. Elegiremos entre *Modo de administración remoto* o *Modo de servidor de aplicaciones*. En el primer caso, sólo será posible que accedan los administradores del sistema para comprobaciones o ejecución de aplicaciones. Como desventaja, se da prioridad a las tareas del propio servidor, con lo que las prestaciones no son muy elevadas. En el segundo caso, se permite a todos los usuarios autorizados conectarse al servidor para la ejecución de aplicaciones. Como ventaja, en este caso el servidor intentará ofrecer las máximas prestaciones a los clientes de Terminal Server. Sin embargo, si optamos por esta segunda modalidad, tendremos que instalar el *Servidor de Licencias de Terminal Server* antes de 90 días, tras los cuales dejará de funcionar el servicio. Si vamos a instalarlo, en la ventana anterior (podremos volver pulsando *Atrás*), tendremos que seleccionar dicho componente entre los disponibles para la instalación. Además, para instalar programas con este modo activado, tendremos



que acudir a *Inicio/Configuración/Panel de Control/Agregar o quitar programas/Agregar nuevos programas*, ya que de lo contrario el sistema operativo nos lo impedirá.
Terminado esto, pulsaremos *Siguiente*, se copiarán los archivos necesarios y se configurarán todos los parámetros seleccionados. En la última pantalla pulsaremos *Finalizar* y podremos empezar a disfrutar de las funcionalidades del Terminal Server.

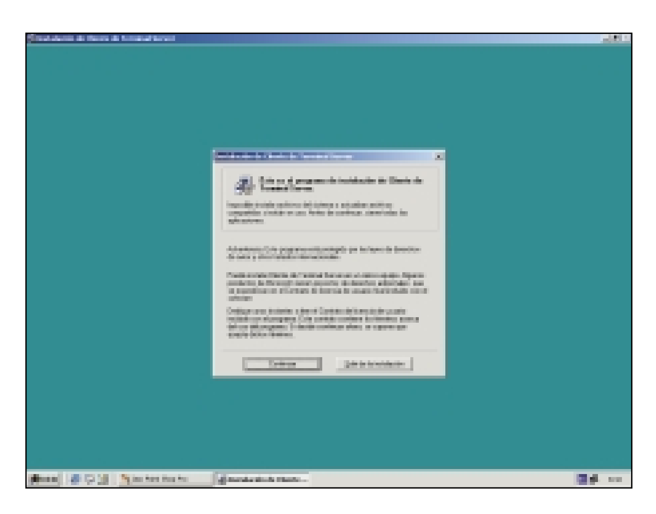
Paso 3
Crear discos clientes



Lo último que tendremos que hacer es crear los discos de instalación para los clientes de Terminal Server, para lo cual no tendremos más que acudir a *Inicio/Programas/Herramientas administrativas/Creador de cliente de Servicios de Terminal Server*. Dependiendo de la plataforma para la que necesitemos crear los disquetes, necesitaremos 2 o 4 discos formateados, y es que existe la posibilidad de que accedamos desde plataformas Windows de 16 bits (Windows 3.x) o 32 bits (Windows 9x/Me/ 2000). Seleccionado el tipo de discos que necesitaremos, pulsaremos sobre *Aceptar*, e iremos insertando uno a uno cada disco cuando nos sea solicitado. Al terminar, estaremos listos para irnos a cada uno de los equipos cliente.

Paso 4
Instalación del cliente

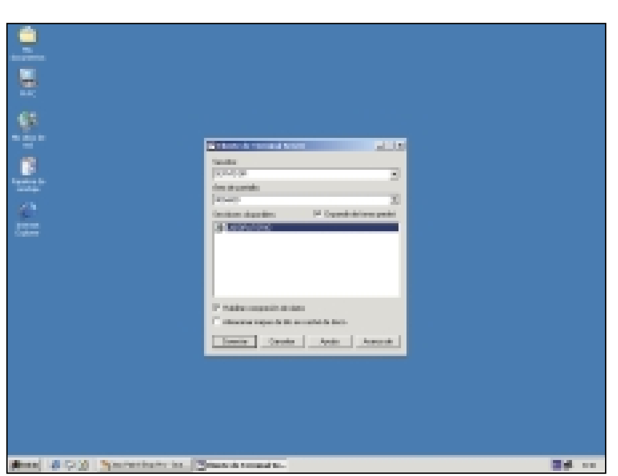
A continuación, acudiremos a cualquier equipo conectado a la red desde el que nos interesa acceder a la ejecución de aplicaciones o administración del servidor remoto. Es importante tener en cuenta que los clientes han de estar configurados en



la red bajo los mismos parámetros que el servidor, es decir, dentro del mismo segmento de direcciones IP que éste y utilizando el protocolo TCP/IP. Además, es posible utilizar equipos conectados a la red mediante *Enrutamiento* o *Acceso Remoto* a través de las líneas telefónicas. Esto abre las puertas a que podamos acceder al *Escritorio* de una máquina remota sin ni tan siquiera estar conectados físicamente a la red de la propia oficina.
Dicho esto, no tendremos más que ejecutar el clásico archivo «setup.exe» del primer disco y seguir un clásico asistente de instalación, donde la única opción que podremos ajustar es el directorio de instalación, y si todos los usuarios tendrán la misma configuración. A esta pregunta, salvo necesidades concretas responderemos con un *Sí*.

Paso 5
Acceso remoto

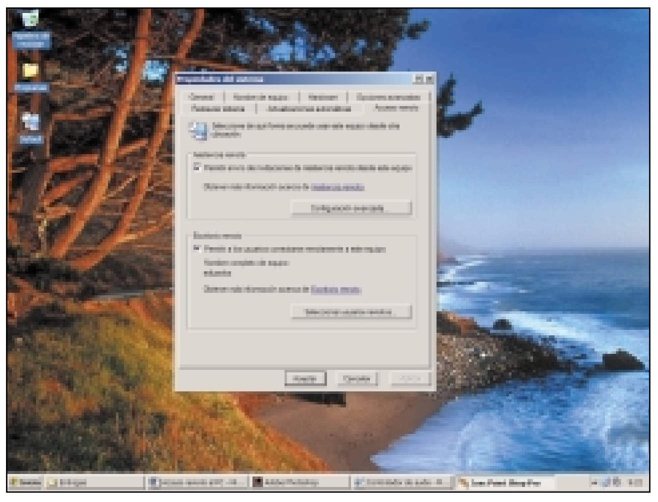
Ahora sólo tendremos que acudir al nuevo grupo que ha aparecido en *Inicio/Programas/Cliente de Terminal Server*, donde pincharemos sobre *Cliente de Terminal Server*. Aparecerá una nueva ventana en la que tendremos que decidir la dirección o nombre del servidor al que nos conectaremos, el tamaño de la pantalla, además de acceder a opciones como la compresión de datos. Respecto al primer dato, salvo que conozcamos la dirección IP del servidor, bastará con introducir su nombre exacto en la red. En cuanto al dato de la pantalla, el tamaño que utilizaremos dependerá de la resolución de la máquina con la que trabajemos. Así, por ejemplo, si empleamos una resolución de 1.024 x 768, lo ideal será utilizar una configuración de 800 x 600, ya que una mayor llenará la pantalla y nos obligará a desplazarnos por el escritorio virtual. Es importante saber que una vez que pulsemos *Conectar*, tendremos una nueva ventana con la que iniciaremos una nueva sesión en el servidor. Esto quiere decir que puede haber múltiples sesiones con aplicaciones distintas, escritorios diferentes, y trabajando en tareas diferentes, sin que en la pantalla del servidor apreciemos nada de esto. Son todo sesiones virtuales que sólo se manejan vía red.



Escritorio Remoto en Windows XP

Paso 1
Ajustes iniciales

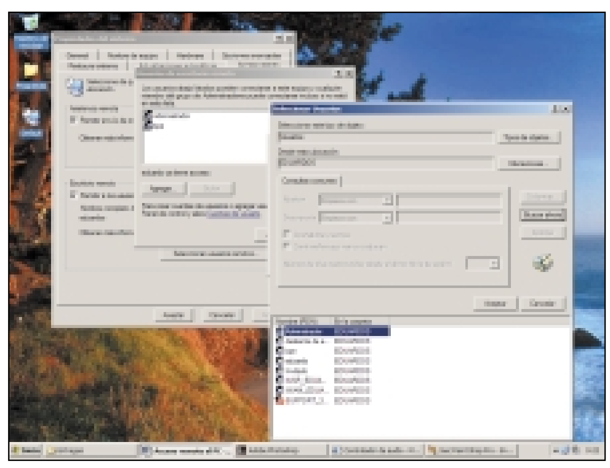
Bajo Windows XP Professional es posible disfrutar de la utilidad del *Escritorio* remoto de manera nativa, es decir, no necesitamos utilizar una versión *Server* para poder acceder a nuestra máquina vía red. Esto tiene sus ventajas y sus inconvenientes. Entre las ventajas, cabe destacar la posibilidad de acceder a casi cualquier máquina de una estructura empresarial sin necesidad de que se trate explícitamente de un servidor. Y, por supuesto, que la funcionalidad se encuentra incluida de manera innata en el sistema operativo, por lo que no tenemos que recurrir a aplicaciones de terceros. Como desventaja frente a la solución de Terminal Server, nos encontramos que, al iniciar la sesión, la máquina cerrará su sesión local, por lo que nadie podrá trabajar mientras tanto con ella.



En cualquier caso, sólo tendremos que acceder a *Inicio/Panel de Control/Sistema* y pinchar en la pestaña de *Acceso remoto*. Aquí tendremos que seleccionar la opción *Permitir a los usuarios conectarse remotamente a este equipo*.

Paso 2
Seleccionar usuarios

Ahora bien, no todo el mundo estará autorizado a acceder a nuestro PC de forma remota. Así, pincharemos sobre el botón *Seleccionar usuarios remotos*. Ante nosotros aparecerá una lista vacía que mostrará los usuarios autorizados. Para completar la lista pulsaremos sobre *Agregar*. En la nueva ventana podremos ir escribiendo los nombres de los usuarios o, mucho más cómodo, buscarlos directamente en la base de datos de usuarios del sistema. Pulsaremos primero sobre *Avanzadas* y después sobre *Buscar ahora*. Abajo aparecerán la lista com-

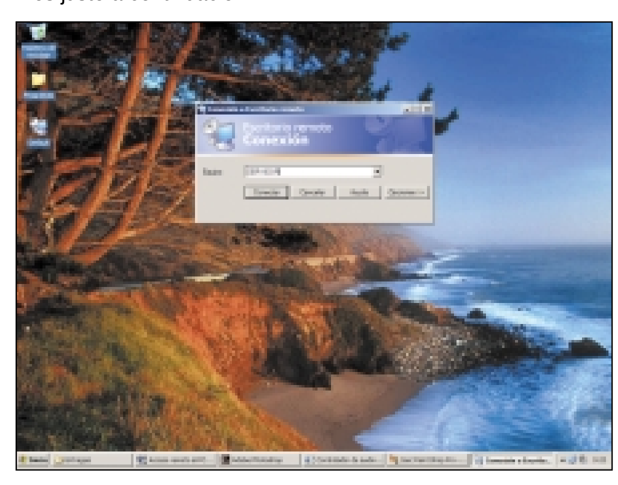


pleta de usuarios del sistema. Seleccionaremos el que nos interesa y pulsaremos *Aceptar*, con lo que se añadirá a la lista. En caso de querer autorizar a varios usuarios, no tendremos más que repetir este proceso.

Cuando terminemos de añadir usuarios, pulsaremos sobre *Aceptar* sucesivas veces hasta salir de todas las pantallas en las que hemos entrado.

Paso 3
Acceso al Escritorio remoto

Llega el momento de probar que el sistema funciona correctamente. Acudiremos a otro equipo en el que también se esté ejecutando Windows XP y tenga correctamente configurada la red. Aquí acudiremos a *Inicio/Todos los programas/Accesorios/Comunicaciones/Conexión a Escritorio remoto*. Con esto tendremos en pantalla una nueva ventana que nos permitirá ajustar multitud de parámetros de funcionamiento que veremos justo a continuación.

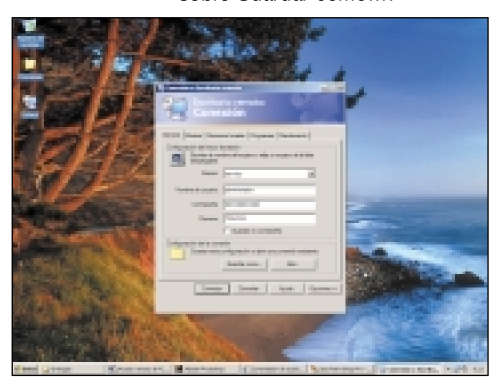


Sin embargo, antes de seguir, es importante dejar claro que con esta utilidad es posible acceder a los Terminal Server de los servidores de Windows 2000, aprovechando las múltiples posibilidades que ofrecen. De esto se deduce que en Windows XP no será necesario instalar los discos de Cliente de Terminal Server que hemos comentado en el Paso 4 del apartado anterior. De la misma forma, es posible, utilizando estos mismos discos del cliente, acceder desde versiones más antiguas de Windows al *Escritorio remoto* de XP. Por ello, si tenemos acceso a estos discos, no será necesario contar con dos Windows XP para poder disfrutar de las capacidades de *Escritorio remoto* de este sistema operativo.

Paso 4
Configurar el Escritorio remoto

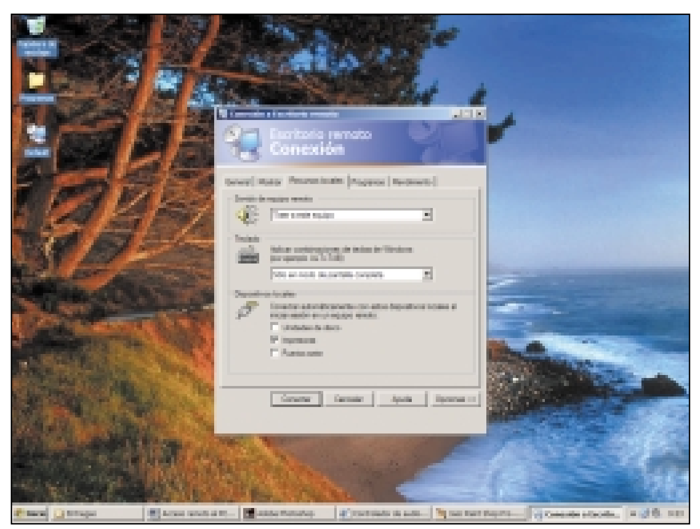
Intermedio

Nos hemos quedado en la ventana de conexión de *Escritorio remoto*. Pero antes de introducir el nombre del equipo y hacer clic sobre el botón *Conectar*, pulsaremos sobre *Opciones*. A continuación veremos cómo se despliega una generosa lista de posibilidades y pestañas de configuración. Para empezar, podremos especificar el nombre y la contraseña, así como el dominio en el que se validarán. Estos datos se guardarán, siempre que marquemos *Guardar mi contraseña*, para futuras conexiones a este servidor. Además, y como dato interesante, si nos interesa guardar un acceso directo a esta conexión en, por ejemplo, el *Escritorio*, no tendremos más que hacer clic sobre *Guardar como…*.



Con la pestaña *Mostrar*, podremos seleccionar el número de colores y tamaño de la pantalla del *Escritorio remoto*. En *Recursos locales* tendremos la oportunidad de traer el sonido y conectar con los puertos y unidades locales desde nuestra máquina, además de poder decidir ciertos ajustes sobre el comportamiento del teclado.

Por último, en *Programas*



indicaremos que se ejecute automáticamente una aplicación al iniciar la sesión remota, mientras que desde *Rendimiento* tendremos la oportunidad de decidir el comportamiento de la conexión dependiendo del medio de conexión utilizado. Así, por ejemplo, podremos omitir la presentación del fondo, animaciones o temas de escritorio. Hemos de tener en cuenta que si la conexión la estamos realizando vía módem o mediante una red lenta o muy congestionada, estos factores pueden ser muy importantes y determinantes para trabajar cómodamente. No podemos olvidar que la cantidad de información que puede ser necesario transmitir es bastante importante, y en casos como estos puede resultar imposible manejar la máquina de manera remota. Ajustadas estas opciones y guardadas si así lo deseásemos, pulsaremos sobre *Conectar* para acceder al *Escritorio remoto* de la máquina especificada.



Acceso remoto

Conectarnos a la red vía teléfono

Intermedio

La tecnología actual hace posible, sin grandes complicaciones, que nuestro servidor permita conectarse de forma remota desde cualquier lugar. De esta manera, podremos ver nuestra red, sus equipos y acceder a todos sus recursos de manera transparente, aunque con un ancho de banda limitado a nuestra línea telefónica. Incluso será posible imprimir vía red en la impresora de la compañía o conectarnos mediante Terminal Server o un programa del estilo de VNC a un escritorio remoto. Es decir, cabe la posibilidad de poner en práctica cualquiera de las cosas que podríamos hacer si estuviéramos conectados físicamente a uno de los cables de red Ethernet de la empresa.

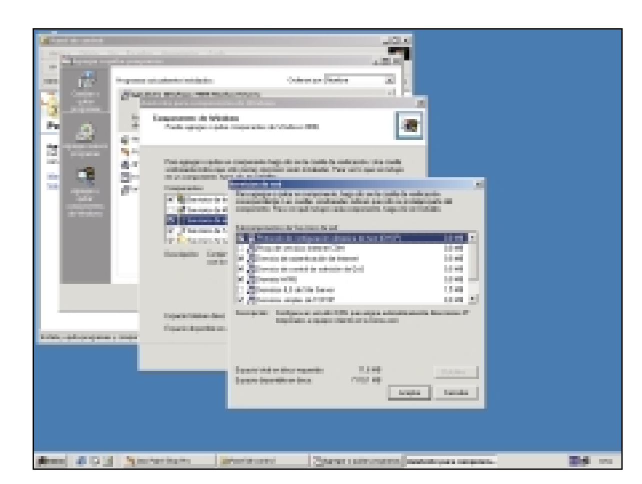
Nuestro práctico va a tratar sobre Windows 2000 Server y sus capacidades de *Enrutamiento y acceso remoto*. La máquina que vamos a utilizar es, además, el controlador del dominio, por lo que gestiona prácticamente todos los procesos de la red. Además, será necesario que instalemos un servidor DHCP para que el enrutamiento funcione correctamente. Este componente es el encargado de configurar automáticamente los clientes que se conecten a la red temporalmente, asignándoles un IP libre, así como los datos de la puerta de enlace y las direcciones DNS.

Por supuesto, damos por hecho que contamos con una línea telefónica, bien sea RTB o RDSI para recibir las conexiones de acceso remoto. Y por supuesto, el servidor tendrá que contar con un módem analógico o digital en exclusiva y permanentemente conectado para poder recibir las llamadas. En cuanto a las líneas, es importante recordar que, si contamos con una RDSI, como es nuestro caso, tendremos que utilizar otra RDSI en el lugar opuesto para poder realizar la conexión. La razón es que los enlaces de datos de esta clase de líneas se realizan de manera exclusiva y directa. Aun así, mediante un conversor digital-analógico es posible recibir llamadas desde un módem convencional sobre una línea RDSI. Sin más, vamos a comenzar a explicar cómo llevar a cabo la instalación.

Servidor DHCP

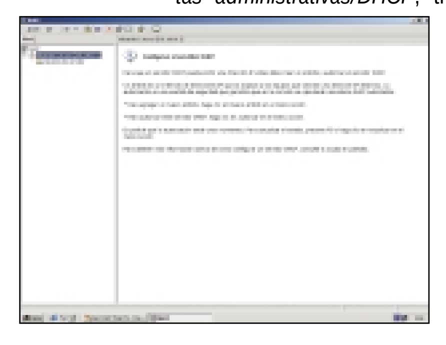
Paso 1
Comprobación inicial

Lo primero que debemos verificar es que el componente se encuentra instalado. Para ello acudiremos a *Inicio/Configuración/Panel de control/Agregar o quitar programas* y pincharemos sobre la categoría *Agregar o quitar componentes de Windows*. En la nueva lista que aparecerá haremos clic en *Servicios de red* y pulsaremos sobre *Detalles*; lo importante es comprobar que el primer componente que nos aparezca en la nueva lista, llamado *Protocolo de configuración dinámica de host (DHCP)*, se encuentra instalado. En caso contrario, lo marcaremos, pulsaremos *Aceptar* y terminaremos el proceso de configuración.



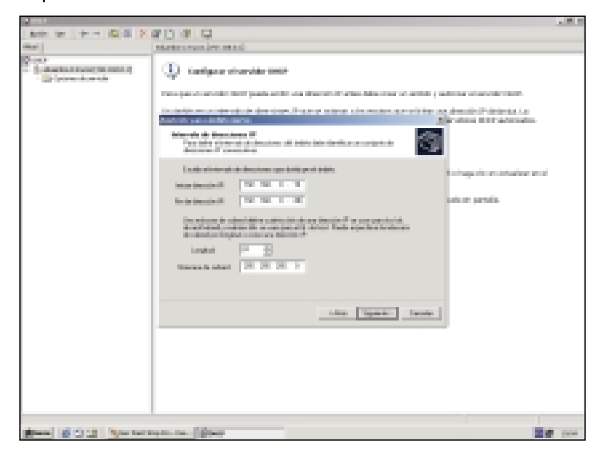
Paso 2
Toma de contacto

A continuación haremos clic en *Inicio/Programas/Herramientas administrativas/DHCP*, tras lo que nos aparecerá una nueva ventana que representa la consola de este servicio. Si hacemos clic sobre el servidor que nos aparece por defecto, es decir, el nuestro, veremos cómo a la derecha nos aparece una larga lista de instrucciones para activar el servicio. Además, vemos que nos aparece junto al nombre un icono rojo que indica que el servicio no esta funcionando.



Paso 3
Crear un ámbito

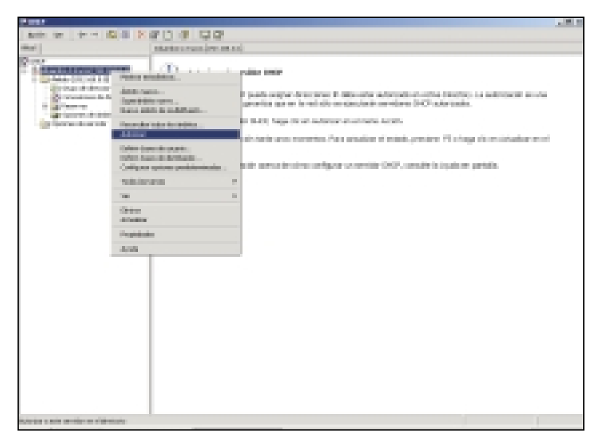
El primer paso para activar el servicio será crear un ámbito. Para ello haremos clic con el botón derecho sobre el nombre del servidor detenido y, en el nuevo menú que aparezca, seleccionaremos *Ámbito nuevo*. Después veremos que aparece un asistente que nos solicita diversos datos. El primero de ellos será el nombre de ámbito, y después el rango de direcciones IP que será utilizado. El número de ellas dependerá de los equipos que preveamos que se van a conectar a la red, dejando siempre 10 o 20 direcciones extras por si acaso. Para cumplimentar este dato es necesario, además, conocer todas las IPs asignadas en la red con el fin de evitar conflictos. En nuestro caso vamos a asignar solamente diez direcciones, ya que el servicio de acceso remoto no va a soportar muchos usuarios.



En los pasos siguientes podremos, sin embargo, excluir direcciones específicas o rangos de ellas, así como indicar el tiempo máximo de asignación de una misma IP a una máquina. Por último, se nos dará la opción de especificar la dirección IP del *router*, así como las direcciones DNS y WINS de la red. Estos datos son imprescindibles ya que, cuando nos conectemos de forma remota, podremos además de navegar por la red, utilizar el *router* para trabajar con Internet. Para finalizar, responderemos que sí a la pregunta de activar el ámbito y pasaremos al siguiente punto.

Paso 4
Autorizar el servidor

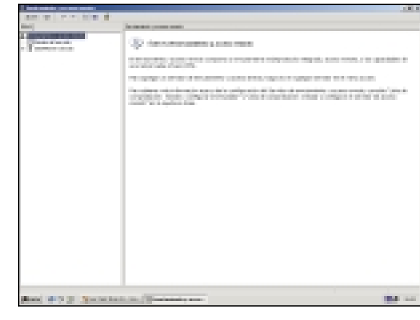
Ahora sólo quedará autorizar al equipo para que comience a funcionar el servidor DHCP. Volveremos a hacer clic con el botón derecho del ratón sobre el nombre del servidor y seleccionaremos la opción *Autorizar*. Esta operación probablemente tarde un buen rato en hacerse efectiva, ya que debe ser el propio *Directorio activo*, es decir, el nuevo concepto de dominio de Microsoft, el que autorice al servidor DHCP para que empiece a funcionar. Entonces veremos aparecer en la parte derecha de la pantalla información de estado. Por otro lado, si desplegamos el ámbito recién creado en la parte izquierda de la pantalla, aparecerán una serie de categorías. En cada una de ellas podemos ajustar diversos parámetros, muchos de los cuales ya elegimos durante el asistente de instalación. Pero además, tendremos la posibilidad de crear directivas de actuación particulares que nos permitan afinar al máximo el funcionamiento del sistema.
En nuestro caso, sin embargo, los datos introducidos son suficientes. A partir de este momento, todo equipo que se conec-



te a la red con las clásicas opciones de *IP asignadas por el servidor*, conectará con este servicio DHCP para que le asigne una IP y le informe de todos los datos de configuración de la red.

Cómo activar un Acceso remoto en Windows 2000 Server

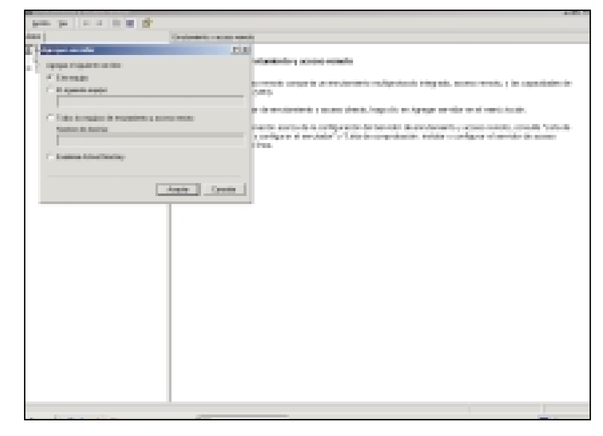
Paso 1
Un primer vistazo



Ahora pasaremos a poner en marcha el servicio de acceso remoto, para lo cual pincharemos sobre *Inicio/Programas/-Herramientas administrativas/Enrutamiento y acceso remoto*. De nuevo tendremos ante nosotros una consola desde la que se gestiona el funcionamiento de este apartado. En la parte de la izquierda se visualizan los servidores disponibles, mientras que en la derecha se mostrarán, en un primer momento, instrucciones para activar el servicio.

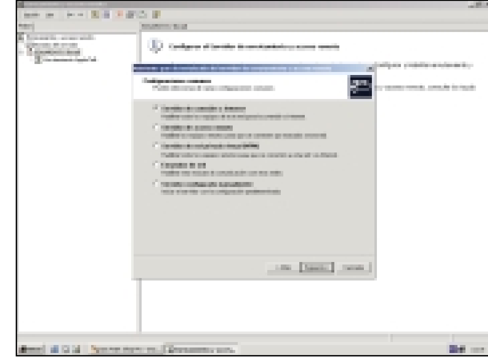
Paso 2
Agregar un servidor

Para poner en marcha el montaje, antes habrá que agregar un servidor que será el encargado de recibir las llamadas de los clientes remotos. Para ello acudiremos al menú *Acción* y pincharemos sobre *Agregar servidor*. En la nueva ventana que aparezca seleccionaremos la opción *Este equipo* y pulsaremos sobre *Aceptar*.



Paso 3
Habilitar servidor

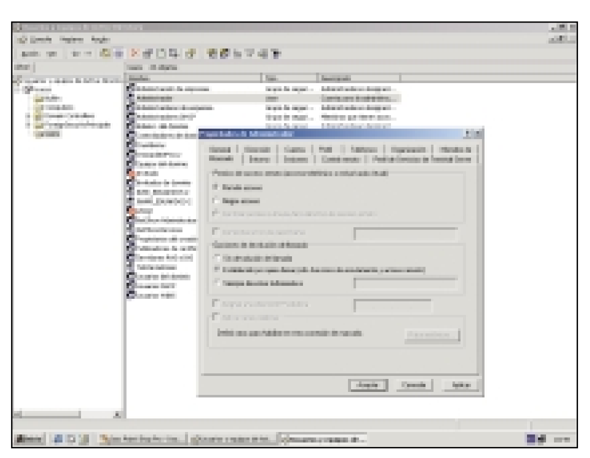
Es el momento de configurar la máquina y habilitar el servicio para lo cual haremos clic con el botón derecho del ratón sobre nuestro servidor. En el nuevo menú contextual que aparezca seleccionaremos la opción *Configurar y habilitar el enrutamiento y el acceso remoto*. Tras esto arrancará un asistente en el que tendremos que ir configurando el servicio. La primera pantalla conflictiva es la que hace referencia a las *Configuraciones comunes*, donde en nuestro caso seleccionaremos la opción *Servidor de acceso remoto* y pulsaremos *Siguiente*. Más tarde comprobaremos que los protocolos utilizados son los que deseamos que utilicen los clientes remotos (pueden ser distintas plataformas), así como tendremos que decidir entre la opción de usar el servicio DHCP o de un intervalo especificado en este momento. Dado que nosotros ya tenemos funcionando este servicio, elegiremos la opción *Automáticamente*.



Algo confusa también puede resultar la pantalla que nos pregunta sobre la utilización de un servidor RADIUS (encargado de la autentificación de usuarios remotos), en la que seleccionaremos la opción *No, no quiero configurar este servidor para usar RADIUS ahora*. Tras esto, sólo nos quedará pulsar *Finalizar* para que el servicio esté en marcha, operación que, dependiendo de la máquina, llevará más o menos tiempo.

Paso 4
Autorizar usuarios

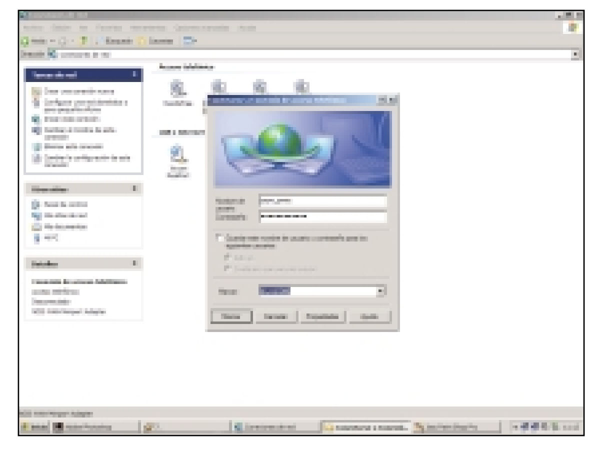
A continuación, tendremos que decidir qué usuarios estarán o no autorizados a utilizar el acceso remoto. Nos dirigimos a *Inicio/Programas/Herramientas administrativas/Usuarios y equipos de Active Directory*. En la nueva ventana que aparezca tendremos que desplegar la lista de opciones que hacen referencia a nuestro servidor en la columna de la izquierda y acudir a la carpeta *Users*. A la derecha aparecerán todos los usuarios del dominio. Ahora haremos clic con el botón derecho sobre cualquiera de los queremos conceder privilegios de acceso, y seleccionaremos *Propiedades*. En la nueva ventana pincharemos sobre la pestaña *Marcado*, donde se



encuentran las opciones del usuario que hacen referencia al acceso remoto.
Para empezar, podremos permitir o negar el acceso y, justo debajo, permitir la devolución de llamada. Esta característica es muy útil para que personas ubicadas en hoteles o en su casa, no deban cargar con el gasto de la llamada de trabajo. El funcionamiento es tan sencillo como que, en caso de estar activada esta característica, nuestra máquina nos preguntará en el momento de la conexión remota si deseamos que nos llame el servidor y a qué número (en caso de que hayamos dado la opción de elegirlo). Seguidamente se desconectará la conexión (que sólo habrá llevado unos segundos), y nuestro equipo se quedará esperando a que el servidor devuelva la llamada.

Paso 5
Conexiones en los clientes

Después de llevar a cabo la configuración de nuestro servidor, sólo quedará que creemos las correspondientes conexiones en nuestra máquina de casa o portátil para acceder desde cualquier lugar. Para realizar esta operación, nosotros hemos utilizado el nuevo Windows XP, aunque la operativa es muy similar sobre Windows 98/Me/2000. Sobre esta plataforma, nos dirigimos a *Inicio/Panel de control/Conexiones de red*, donde seleccionaremos la opción *Crear una conexión nueva* de la columna de la izquierda. A continuación arrancará un asistente en el que iremos introduciendo los distintos datos. Sin embargo, el punto decisivo lo encontraremos en el momento en que lleguemos a la segunda pantalla, donde tendremos que elegir el tipo de conexión que deseamos utilizar. En nuestro caso, seleccionaremos la opción de *Conectarse a la red de mi lugar de trabajo*, para después especificar que lo queremos hacer mediante una *Conexión de acceso telefónico*. Indicaremos qué dispositivos son los que realizarán el marcado, asignaremos un nombre y un número de teléfono y la conexión estará creada.



Ahora, tras hacer doble clic sobre ella en la ventana de *Conexiones de red*, bastará con que introduzcamos un nombre de usuario y contraseña válidos ya autorizados así como el número de teléfono correcto y pulsemos *Marcar*. Si tenemos activada la posibilidad de la devolución de la llamada, en breves momentos, tras comprobar nuestro nombre de usuario y contraseña, se nos preguntará si deseamos que nos llame el servidor. En caso de ser así, introduciremos el número de teléfono completo y pulsaremos *Aceptar*, en caso negativo, *Cancelar*. En cualquier caso, una vez terminado el proceso, bastará con acudir al *Entorno de red* para ver cómo estamos integrados dentro de la red de la empresa, al tiempo que podemos acceder a sus recursos, aunque con un ancho de banda bastante limitado.



Tiendas on-line

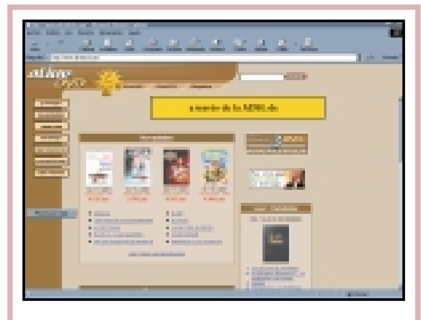
Ventajas de comprar todo tipo de artículos de ocio desde el PC

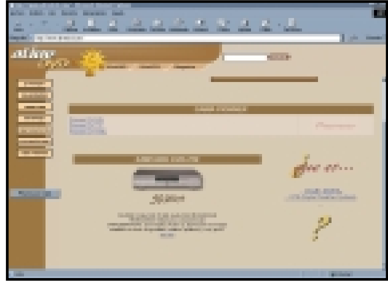


Han transcurrido ya varios años desde que Internet se acercase por primera vez al hogar de los usuarios españoles. Cada consumado cibernauta de los muchos que en la actualidad navegan a través de la Red se ha acercado a este popular mundo de una forma muy particular. Pero lo realmente importante no es cómo ha llegado hasta nosotros Internet. Ni siquiera el tiempo que llevamos utilizándolo. Lo que verdaderamente importa es la utilización que cada usuario hace de los recursos que la Red pone a su disposición, el beneficio que obtiene de esta emergente tecnología. Si le preguntásemos a un usuario cualquiera qué es lo que representa Internet para él, probablemente contestaría que significa el acceso a un mundo repleto de información, de conocimiento. Pero la Web no es sólo eso. Hace más cómoda nuestra vida. Pone al alcance de nuestra mano, desde nuestra propia casa, un sinfín de posibilidades que otrora requerirían que nos desplazásemos al banco, al mercado, a la universidad. Por supuesto, estamos hablando del comercio electrónico. Gracias a este ingenioso invento es posible comprar prácticamente cualquier cosa desde el sillón de nuestra casa. Y no a ciegas. Viéndolo, conociendo sus características, adquiriéndolo con garantías y con comodidad. Sin embargo, parece que el *e-business*, al menos en nuestro país, no termina de cuajar. ¿Por qué? Muy sencillo. Porque no nos fiamos. Porque introducir el número de nuestra tarjeta de crédito a través del teclado de nuestro ordenador y enviarlo a saber dónde no nos parece seguro. Estamos en nuestro derecho. Es lógico que cada persona proteja sus intereses. Sin embargo, lo que muchos usuarios quizás no sepan es que las grandes empresas implicadas en este fenómeno, de telecomunicaciones, importantes desarrolladores de software, han realizado inversiones multimillonarias para que el hecho de efectuar estas transacciones no implique ningún riesgo. Para que sea seguro y protegernos de esos a los que algunos llaman piratas. O *hackers*.

En la actualidad, las compras *on-line* no son lo que eran. Ahora son mucho más seguras. Por supuesto, nunca podremos afirmar que son del todo infalibles, pero ahora estamos mucho más cerca de conseguir esa ansiada seguridad total a través del cifrado. Una sencilla, a priori, técnica que transforma una determinada información en otra ininteligible por todo aquel que no deba conocerla y que nos proporciona seguridad. Nos permiten contratar ese viaje tan ansiado, conseguir el último lanzamiento discográfico de Sting adquiriéndolo directamente en Estados Unidos, matricularnos en la universidad, todo ello desde casa. Y gracias a la tecnología SSL (*Security Socket Layer*). La que en su interior esconde eso que hemos mencionado anteriormente, a la que los que más saben llaman cifrado. La que sí es soportada por nuestro navegador, y también por el servidor al que nos estamos conectando, garantiza nuestra privacidad. Que el número de nuestra tarjeta de crédito tan sólo será utilizado para lo que nosotros queremos: para pagar el importe de nuestra compra.

A lo largo de las siguientes páginas recorreremos un sinfín de posibilidades: podremos adquirir libros, discos de música, ordenadores, juegos de ordenador y de videoconsola, en España y en el extranjero. Y lo que es más importante, de forma segura, tanto en pequeños negocios caseros como en grandes cadenas que han descubierto las bondades de Internet. Porque la Red es algo más que un negocio y está, o debería estarlo, al alcance de todos.





AliveDVD

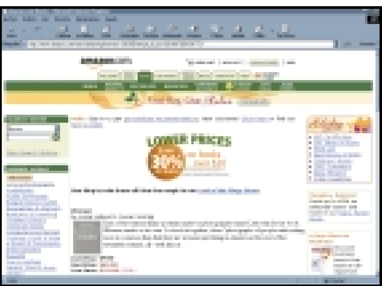
www.alivedvd.com

Son muchos los cibernautas que comparten su pasión por la informática con su afición al cine doméstico. Pensando precisamente en ellos, son también muchas las tiendas virtuales que han aparecido en Internet ofreciendo lo mejor del *home theatre* al mejor precio. Y en este ámbito, AliveDVD es una de las más populares. Gracias a una simple y eficaz interfaz, comprar *on-line* cualquier novedad lanzada en formato DVD resulta una tarea realmente sencilla. Un catálogo enormemente amplio garantiza al cliente la obtención de prácticamente cualquier título editado en este formato. No obstante, quienes aún no tengan un equipo capaz de reproducir películas en formato DVD, pueden optar por su completa sección de títulos en el ya clásico formato VHS, otra de las posibilidades ofrecidas por este *site* a sus clientes.

El sistema de reservas previas a la fecha de lanzamiento de los títulos permite a los usuarios más impacientes disponer de sus filmes favoritos tan pronto como aparezcan en el mercado, beneficiándose además de importantes descuentos. Por si todo esto fuera poco y para completar una más que interesante oferta, AliveDVD pone a disposición de sus clientes una promoción semanal que incluye tres películas a un precio inmejorable.

Las formas de pago disponibles para todos los envíos nacionales son abono con tarjeta de crédito, ingreso en cuenta y pago contrareembolso. Para garantizar la privacidad de los datos de los consumidores la página está alojada en un servidor seguro que integra tecnología SSL.





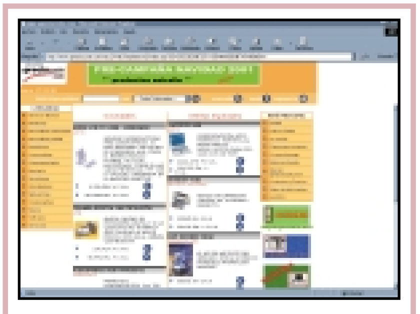
Amazon.com

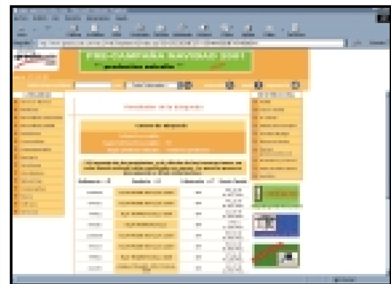
www.amazon.com

Si alguna de las tiendas *on-line* que encontraréis en este artículo goza de una popularidad tal que no precisa presentación alguna es, sin duda, Amazon.com. En este gigantesco portal podemos encontrar todo tipo de artículos de ocio: desde la última edición del *best-seller* de moda hasta el más avanzado reproductor de películas en formato DVD disponible en el mercado. Pero eso no es todo. Música, electrónica, juegos, software, revistas o fotografía son sólo algunas de las categorías representadas por multitud de productos, normalmente a precios realmente competitivos. Pero Amazon representa algo más para los cibernautas españoles, ya que es la forma más cómoda de adquirir artículos importados directamente desde Estados Unidos o Japón, productos que en algunos casos no es posible encontrar en España.

Para garantizar la absoluta seguridad de las transacciones que efectúan sus clientes, Amazon dispone de servidores SSL que integran el que en la actualidad es el mejor software de seguridad para realizar compras *on-line*.

Desafortunadamente y a pesar de que la compañía cuenta con filiales internacionales situadas en Europa, concretamente en el Reino Unido, Francia y Alemania, los hispanohablantes no podemos acceder, al menos por el momento, a sus contenidos traducidos a nuestro idioma. Igualmente es conveniente informarse, antes de realizar un pedido, de los costes de envío del producto, dado que previsiblemente será enviado desde alguno de estos países.





A precio coste

www.apreciocoste.com

Comprar productos informáticos directamente desde el PC del cuarto de estar es ahora posible gracias a tiendas virtuales como A precio coste. Su completísimo escaparate abarca todo tipo de artículos, tanto hardware como software, lo que a buen seguro situará este *site* entre las opciones preferidas por los adictos a la informática. Además no debemos olvidar que, tal y como reza el nombre de este portal, los precios de los artículos son más que razonables, por lo que su consulta es cuanto menos recomendable.

Gracias a su sencilla interfaz, que agrupa los productos por categorías, es realmente fácil localizar cualquier artículo.

Uno de los servicios que merece la pena destacar es el de atención al cliente, disponible en horario comercial, a través del que personal especializado solventará todas las consultas de los clientes.

Como viene siendo habitual en las empresas que centran su actividad de negocio en el comercio electrónico, ofrece múltiples fórmulas de pago a sus clientes. Los particulares pueden abonar el coste de su pedido realizando un ingreso directo en la cuenta bancaria de A precio coste, aunque también pueden optar por la transferencia. Las empresas, además de estas dos opciones, pueden abonar el importe de los pedidos pagando a posteriori, lo que supone un incremento del 1,5% en el precio de los productos. En definitiva, un completo portal cuya amplia gama de productos satisfará las necesidades tanto de particulares como de empresas.



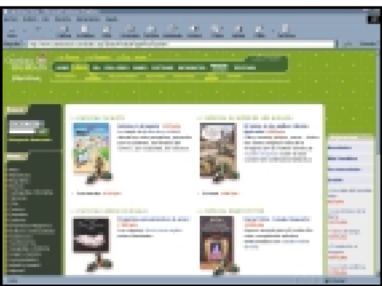


AreaPC

www.areapc.com

De nuevo nos topamos con una tienda virtual especializada en todo tipo de componentes y sistemas informáticos aunque, en este caso, la organización de su escaparate difiere de la utilizada por otros portales que centran su actividad de negocio en el mismo tipo de productos. Para facilitar a sus clientes la localización de los artículos buscados, AreaPC los agrupa en varias tiendas especializadas en los distintos fabricantes que aglutinan los componentes de mayor calidad. Compaq, Hewlett Packard, Epson, IBM o Canon, son tan sólo algunos de los muchos gigantes del sector presentes en el escaparate de este *site*. Igualmente merece la pena destacar su amplísima oferta de consumibles, característica que sitúa a esta web en una posición aventajada frente a otras que no dan toda la importancia que merecen este tipo de productos. Pero lo que sin duda más agradará a los posibles clientes de AreaPC son los suculentos descuentos que el portal pone a su disposición: descuentos financieros de hasta un 2% del importe del pedido, descuentos comerciales variables en función del producto adquirido, e incluso cabe la posibilidad de ahorrar un 1% del importe total utilizando un teléfono móvil para validar la transacción. A esta última e innovadora modalidad de pago conocida como PayBox le espera, con el beneplácito de los consumidores, un futuro halagüeño gracias al apoyo de importantes entidades financieras, como Deutsche Bank.
La garantía que ofrece AreaPC a sus clientes es la privacidad de los datos y la posibilidad de devolver los productos adquiridos durante los siete días posteriores a su compra.

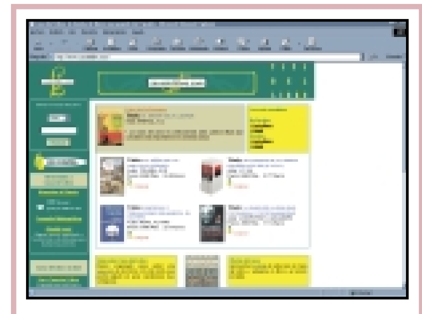


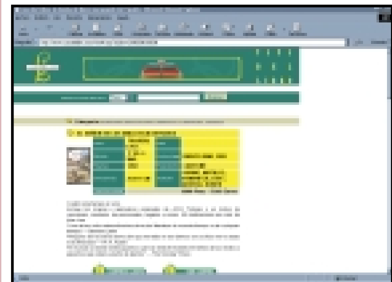


Carrefour Ocio

www.carrefourocio.com

La presencia en Internet de los grandes centros comerciales no data precisamente de fechas recientes. El atractivo de ampliar su oferta haciéndola llegar a los muchos usuarios de la Red es evidente, máxime cuando se trata de compañías de la envergadura de El Corte Inglés, la FNAC o Carrefour. Si algo caracteriza al portal diseñado por esta última empresa para dar a conocer su amplio catálogo de artículos a la comunidad cibernauta es sin duda la gran sencillez de su interfaz, superior a la de la mayor parte de las tiendas virtuales de este mismo artículo. Gracias a las innumerables categorías que encontraremos en el marco situado en la zona izquierda de la ventana de nuestro navegador favorito, acceder al producto buscado es coser y cantar. Y, precisamente, no porque la cantidad de artículos ofertados sea pequeña. En esta web Carrefour Ocio pone a disposición de sus clientes una variada oferta bibliográfica, multitud de CDs musicales, películas en formato DVD, accesorios de telefonía móvil y, en definitiva, todo tipo de artículos relacionados con el mundo del ocio.
Como viene siendo habitual en los espacios virtuales de las grandes compañías como la que ahora nos ocupa, el cliente puede negociar los plazos de entrega que más les convenga ajustándose, lógicamente, a la disponibilidad del material en el almacén de Carrefour Ocio.
A las formas de pago habituales en los portales destinados al comercio electrónico la compañía francesa añade su propia tarjeta, conocida como Pass, que permite al cliente, entre otras posibilidades, obtener créditos de forma automática.





Casa del Libro

www.casadellibro.com

La Casa del Libro ha sido y es en la actualidad un lugar de referencia para todos los amantes de la lectura en nuestro país. El principal aval de las diferentes sucursales establecidas en las principales capitales del territorio español es, por supuesto, su descomunal fondo bibliográfico. Y, precisamente, esto es lo que la tienda virtual de este popular establecimiento pone al alcance de todos los aficionados a la lectura con acceso a Internet.
Localizar un volumen determinado es realmente sencillo. Para ello, únicamente hay que utilizar el índice temático a través del cual el cliente tiene acceso a la categoría bibliográfica a la que pertenece el libro. Otra forma realmente eficaz de localizar un volumen concreto es utilizar el buscador integrado en la interfaz. Una vez asegurada su disponibilidad, completar el proceso de adquisición se reduce únicamente a suministrar los datos del cliente necesarios para proceder al envío y cobro del libro.
El interés por este portal bibliográfico se ve acrecentado si tenemos en cuenta que, a través de éste, podremos acceder a otras opciones que contribuyen a ampliar el valor añadido de los servicios ofertados a sus clientes. Los mejores ejemplos son el foro y la sección dedicada a la información acerca de la actualidad literaria, dos nuevos motivos para visitar esta página.
Obviamente, la seguridad de las transacciones no ha sido descuidada. El algoritmo de cifrado RSA utilizado por el protocolo SSL garantiza la privacidad de los datos de todos los clientes de esta tienda virtual.





Centro MAIL

www.centromail.es

El portal de esta cadena especializada en informática y videojuegos es posiblemente uno de los más completos y competitivos del mercado español, sobre todo en este último sector, los videojuegos. Son muchos los años de experiencia de esta cadena, anteriormente conocida como Mail Soft, lo que sin duda alguna se aprecia en la calidad del portal con el que ponen a disposición de la comunidad cibernauta su amplia gama de productos. La web ha sido estructurada a partir de las diferentes plataformas a las que van dirigidos los productos comercializados por la tienda virtual. Adquirir un juego para PC, PlayStation 2, Game Boy Advance, Dreamcast o cualquier otro sistema disponible en la actualidad, es realmente sencillo gracias a su elaborada pero intuitiva interfaz.

Las distintas formas de pago que los usuarios tienen a su disposición abarcan desde el envío a través de una agencia de transporte urgente, para pedidos peninsulares o desde las islas Baleares, hasta la recepción vía correo postal, en el caso de los clientes que residen en las islas Canarias, Ceuta, Melilla o Portugal.

La seguridad y confidencialidad de la información suministrada por los clientes están garantizadas gracias a la utilización de servidores SSL, y del cumplimiento de lo establecido por la Agencia de protección de datos. Centro MAIL también garantiza que las *cookies* generadas por sus servidores son incapaces de leer información del disco duro instalado en el PC del cliente. Sin duda alguna, las posibles carencias de seguridad tan temidas por muchos usuarios a la hora de realizar una compra *on-line* han sido resueltas por esta cadena de forma eficaz.



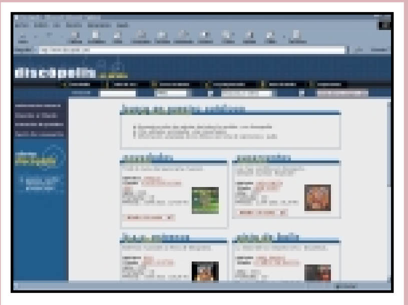


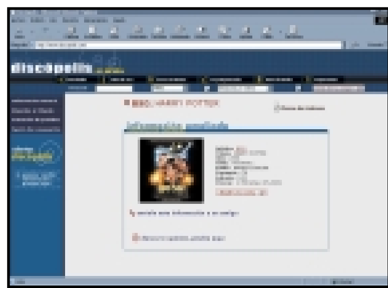
DiscoLibro

www.discolibro.com

Como se puede intuir a partir de su nombre, esta tienda virtual dispone de una de las mayores ofertas discográficas al servicio de los cibernautas hispanohablantes, aunque en ella también encontraremos un completo fondo bibliográfico capaz de satisfacer a los aficionados a la literatura más exigentes. La variedad de los géneros musicales disponibles es realmente amplia: blues, soul, música clásica, jazz, *new age*, pop, country, folk, etc. En lo referente al apartado bibliográfico, la oferta no es menos imponente: filosofía, informática, psicología, archivística, derecho, economía, educación o ciencias exactas son sólo algunos de los géneros que encontraremos en su completo escaparate. Para acceder a cada uno de estos géneros, tanto en el apartado musical como en lo referente a los libros, tan sólo es necesario hacer clic en el hiperenlace correspondiente, estando situados todos ellos en una lista ubicada en un marco en la parte izquierda de la ventana del navegador. Tal y como viene siendo habitual en este tipo de portales, es posible efectuar la búsqueda de un producto concreto utilizando el motor de búsqueda al que tendremos acceso desde la pantalla inicial de la interfaz.

Una de las áreas temáticas de DiscoLibro está orientada a ayudar a los usuarios indecisos en esas situaciones en las que el cliente no sabe exactamente qué es lo que busca. Basta con dirigirse a la pestaña *Regalos* para acceder a un sinfín de posibilidades, todas ellas con la garantía y la experiencia de esta tienda virtual.





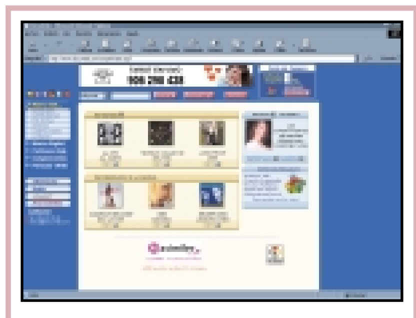
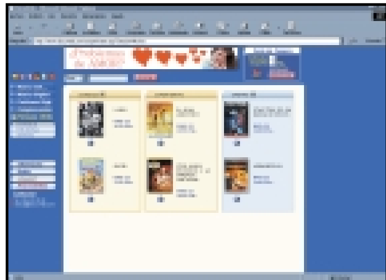
Discopolis

www.discopolis.com

Las posibilidades de la Red en todo lo referente a la compra de CDs musicales son enormemente amplias. Buena prueba de ello es esta página, que viene a unirse a la enorme oferta en este sector aportando un amplio catálogo y una interfaz muy elaborada que agradará a todos sus clientes. Los géneros musicales que encontraremos en Discopolis abarcan prácticamente todos los disponibles a nivel mundial: desde el jazz más actual hasta los grandes éxitos de la música pop, pasando por las bandas sonoras originales de las películas más populares de la cartelera cinematográfica. En su interfaz encontraremos accesos directos a los géneros más demandados aunque, sin lugar a dudas, los enlaces más interesantes para los usuarios son aquellos que hacen referencia a los «superventas» y a las «ofertas». Y es que, por supuesto, la tienda virtual pone a disposición de todos sus clientes una amplia gama de productos a un precio inmejorable. Eso sí, una oferta limitada a las unidades en *stock*.

La localización de un producto musical concreto se realiza a través de una completa herramienta de búsqueda que utilizará, como claves de ubicación en la base de datos de Discopolis, el nombre del artista y el estilo musical al que pertenece el volumen en cuestión.

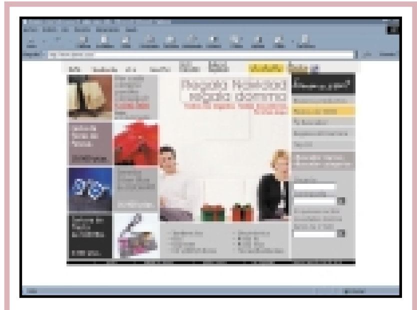
Este completo portal dedicado a los muchos cibernautas amantes de la música dispone de un servicio de información *on-line* al que pueden suscribirse todos los clientes interesados en permanecer informados acerca de las ofertas del panorama musical, por supuesto, de forma totalmente gratuita.

DiscoWeb

www.discoweb.com

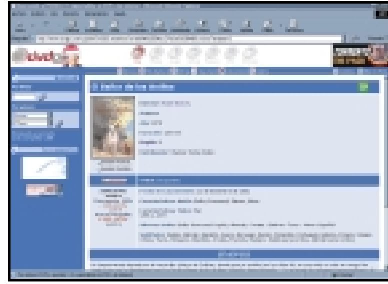
Nos encontramos ante una de las tiendas virtuales más completas al servicio de los usuarios hispanohablantes. Y es que, en este caso, los responsables de este portal se han percatado de las enormes posibilidades que ofrece el hecho de acercar su oferta a los muchos cibernautas que utilizan la lengua de Cervantes, ya que, además del español, el *site* utiliza otras lenguas como el inglés, francés o alemán, lo que da una idea de la envergadura de la infraestructura que subyace bajo sus servidores.
En el escaparate de DiscoWeb encontraremos una amplísima oferta musical, todo tipo de complementos, los mayores éxitos cinematográficos en formato DVD; en definitiva, un mundo de ocio al alcance de todos los aficionados a la informática que dispongan de algún tipo de acceso a Internet. Pero la oferta de este imponente portal no concluye aquí. Y es que los aficionados a la música más duchos tienen la posibilidad de adquirir las partituras de sus composiciones musicales preferidas, todo con la sencillez que caracteriza a las tiendas virtuales de última generación.
Obviamente, y al igual que sucede en el resto de portales que os presentamos en este artículo, todas las compras se realizarán bajo las más estrictas condiciones de privacidad, ya que DiscoWeb utiliza servidores seguros capaces de establecer con nuestro navegador un proceso de comunicación basado en el protocolo SSL (*Security Socket Layer*). Toda una garantía.




Dommo

www.dommo.com

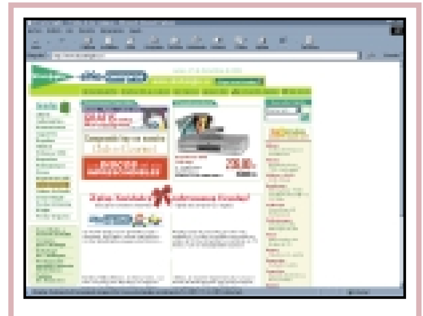
Dommo es algo más que un portal destinado al ocio. Es un mundo orientando a dar a conocer a sus clientes las últimas tendencias, el apasionante universo de la electrónica, la moda, los regalos, lo mejor del panorama musical, etc. Pero su oferta no acaba aquí. Objetos tan necesarios en algunas ocasiones como una caja de bombones o un ramo de flores también están a nuestra disposición gracias a este original *site*. Sin duda, un sinfín de posibilidades.
El diseño de la interfaz rompe con lo visto anteriormente, asemejándose en esta ocasión más a un catálogo impreso en papel que a una página web, lo que sin duda facilita su utilización por parte de los usuarios con menos experiencia a la hora de acceder a las múltiples posibilidades de la Red.
Hacer un regalo nunca ha sido tan sencillo. Dommo ofrece montones de sugerencias, de todos los tipos y orientadas a un sinfín de personas, algo que sin duda agradecerán los muchos usuarios que se enfrentan a la difícil decisión de encontrar una sorpresa adecuada. Pero si el cliente tiene las ideas totalmente claras, encontrar el objeto buscado no podría ser más sencillo, ya que es posible utilizar una herramienta de búsqueda que lo ubicará de forma automática.
Con el fin de proporcionar las máximas condiciones de seguridad a sus clientes, Dommo utiliza servidores seguros capaces de cifrar la información que los usuarios suministran al portal, manteniéndola protegida del acceso de terceros.

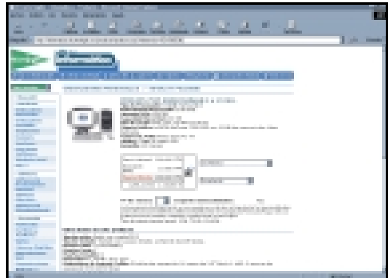



DVDGo

www.dvdgo.com

Si te apasiona el *home theatre*, esta es tu tienda virtual. En DVDGo encontrarás todas las películas que han sido editadas en formato DVD, a los mejores precios. Y no sólo eso. Esta tienda virtual ofrece la posibilidad de reservar un título con antelación a su fecha de lanzamiento, lo que garantiza su disponibilidad en el mismo momento en que llegue a las estanterías de las tiendas especializadas.
Pero el enorme atractivo de este portal no acaba aquí. Su cuidada interfaz pone al alcance de un clic de ratón información acerca de los títulos más vendidos, todo tipo de noticias acerca del panorama cinematográfico y del versionado de los films más populares a formato digital, un sinfín de recomendaciones y grandes ofertas. Para amenizar la visita de sus clientes, DVDGo cuenta con la colaboración de estrellas del mundo televisivo y cinematográfico de la talla de Santiago Segura, el Gran Wyoming o Pablo Carbonell, personajes que, con la gracia que les caracteriza, nos obligarán a esbozar una sonrisa a la par que nos ofrecen su visión acerca de la oferta actual del mundo de las películas en formato DVD.
En lo referente a la seguridad que esta tienda virtual ofrece a todos sus clientes, cabe mencionar que el *site* cuenta con la certificación *VeriSign*, lo que garantiza la más estricta confidencialidad de todos los datos que nuestro navegador envíe a los servidores de la tienda *on-line*.





El Corte Inglés

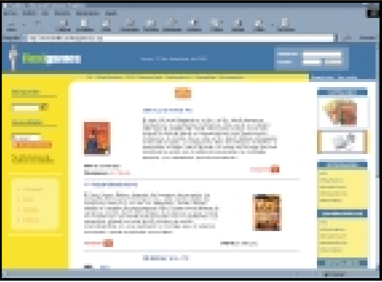
www.elcorteingles.es

Nos encontramos ante uno de los portales en los que toda presentación huelga. Si existe una cadena de grandes establecimientos sobradamente conocida por todos los españoles, es sin duda El Corte Inglés. La cantidad de productos que es posible adquirir a través de su portal en Internet es sencillamente abrumadora. Libros, artículos de informática, juguetes, regalos, música, videojuegos, deportes y vinos son tan sólo algunos de los artículos que incluye su descomunal oferta. Pero esta enorme variedad no es todo lo que los clientes pueden obtener de esta web. Y es que todos los productos adquiridos en la tienda *on-line* de esta prestigiosa cadena de centros comerciales cuentan con la garantía que ha venido avalando a la compañía a lo largo de su historia. Y no hablamos tan sólo de calidad. También de la posibilidad de cambio o devolución. Además, los clientes que posean la tarjeta emitida por esta entidad se beneficiarán de todas las ventajas que ésta ofrece en cuanto a facilidades de pago.

La interfaz de este *site* ofrece la posibilidad adicional a sus clientes de suscribirse a boletines informativos, de comprar productos por catálogo, utilizar su tablón de anuncios y beneficiarse del envío de catálogos totalmente gratuitos a su domicilio particular.

En definitiva, una tienda virtual avalada por la larga trayectoria de una de las principales cadenas de centros comerciales ubicadas en España. Toda una garantía de experiencia y saber hacer.





Flexiline

www.flexiline.es

En esta ocasión no nos encontramos ante la web de una compañía especializada únicamente en la venta *on-line* de artículos. Flexiline es una empresa que, además de contar con dos tiendas virtuales, una especializada en hardware informático y la otra en videojuegos, se dedica a la investigación y desarrollo en el ámbito de las tecnologías de la información y al ensamblaje de equipos informáticos, con su posterior distribución y comercialización.

Desde esta web, los clientes pueden configurar su propio ordenador personal de acuerdo a sus necesidades, pero si prefieren adquirir un equipo previamente definido, Flexiline pone a su entera disposición un amplio abanico de posibilidades, con configuraciones que abarcan desde los PC más sencillos hasta los servidores más potentes. Pero su extensa oferta no acaba aquí. A través del portal Flexigames, los cibernautas tendrán acceso a un sinfín de productos relacionados con el universo de la informática lúdica. Las plataformas que se encuentran representadas abarcan tanto el terreno de las consolas de videojuegos como el de los ordenadores compatibles. Si tienes una PlayStation, una Nintendo 64, una Dreamcast, una PS2, una GameBoy o un PC, esta es tu página.

Para completar una oferta de lo más atractiva, Flexigames organiza todo tipo de concursos, permite la descarga de demos de los productos software y pone a disposición de sus usuarios múltiples foros en los que debatir acerca del panorama lúdico que tantos adeptos tiene en nuestro país.



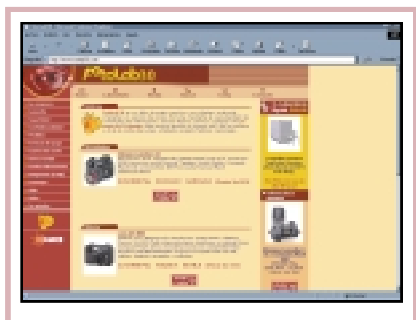
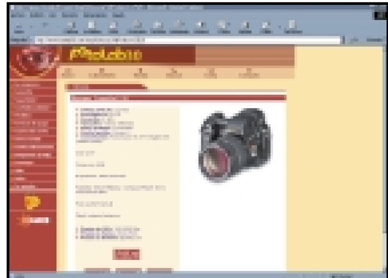


FNAC

www.fnac.es

Sin lugar a dudas, la FNAC es uno de esos centros comerciales que, en un tiempo récord, se ha ganado la confianza de miles de españoles amén de un amplio surtido de productos y una atención de calidad. Para diversificar su oferta, presente ya en la mayor parte de las grandes ciudades españolas, hace ya tiempo que puso en marcha su propio portal, a través del cual es posible adquirir cualquiera de los productos que podemos encontrar en las vitrinas de sus establecimientos. Estos artículos comprenden libros, discos, películas en formato DVD y VHS, software, hardware, entradas para conciertos, etc.

La interfaz de esta tienda virtual goza de la elevada calidad que exige un centro de estas características, resultando muy intuitiva y simplificando notablemente la localización de cualquier producto ofertado por la compañía a través de un sencillo buscador. Lógicamente, la empresa garantiza no sólo la total confidencialidad de la información suministrada por sus clientes, sino también los mejores precios, unos plazos de entrega previamente fijados y la garantía de satisfacción de los productos adquiridos. También es posible reservar un producto para que éste sea recogido posteriormente en la tienda, evitando de esta forma desplazamientos innecesarios y simplificando la compra a los clientes que prefieran personarse para recoger los artículos. En resumen, un completo espacio virtual que viene a sumarse a la amplia oferta disponible aunando variedad, calidad y el respaldo de una de las empresas que, a pesar de su aún corta experiencia en nuestro país, cuenta ya con la confianza de muchos aficionados a la cultura en sus diversas manifestaciones.

FotoLab30

www.fotolab30.com

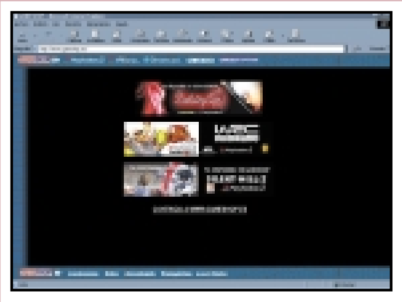
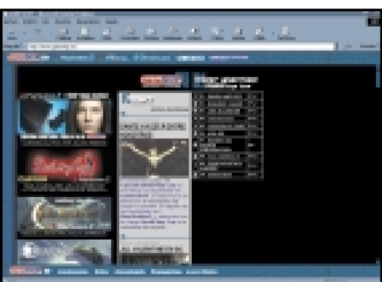
La fotografía digital es una afición que ha pasado, en un período de tiempo muy reducido, de estar al alcance de unos pocos privilegiados a poder ser utilizada prácticamente por todo el mundo. El motivo: la reducción de los precios de las cámaras digitales y la popularización de Internet, uno de los motores y principal transmisor de este tipo de fotografías. Por este motivo, son muchas las tiendas virtuales que están apareciendo en la Red para responder a las demandas de los consumidores. Una de las más completas es, sin duda alguna, la que ahora nos ocupa.

FotoLab30, una empresa con gran experiencia en este sector, oferta todo tipo de cámaras digitales, servicios de revelado, cámaras *reflex* convencionales, en definitiva, una amplia variedad de productos relacionados con el mundo de la fotografía.

Las formas de pago que acepta esta tienda virtual son básicamente tres: tarjeta de crédito, transferencia bancaria y pago contra reembolso.

En el apartado dedicado al laboratorio, explican detalladamente la cuidada metodología que utilizan a la hora de realizar el proceso de revelado. Todo un detalle que sabrán apreciar los aficionados a la fotografía más exigentes.

En la página principal del *site* está disponible un enlace en el que la compañía explica a sus clientes las medidas de seguridad que utilizan para garantizar la total privacidad de la información de éstos. Sin duda, una buena iniciativa que contribuirá a tranquilizar a los consumidores que miran con más recelo hacia el mundo del comercio electrónico.

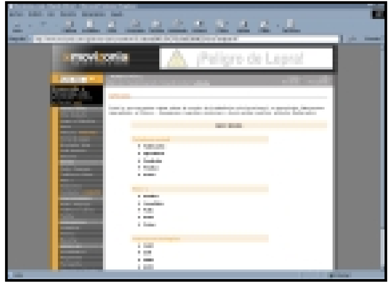
GameSHOP

www.gameshop.es

El mercado de los videojuegos, tanto para la plataforma PC como para consolas, es tan competitivo como rentable para las gigantescas compañías que lo lideran. Nuestro país es un ávido consumidor de este tipo de productos, y por este motivo son muchas los portales en los que se oferta información sobre las últimas novedades en este campo, e incluso se comercializan los títulos más novedosos.

En GameSHOP encontraremos todas las novedades desarrolladas para las plataformas que pueblan el mercado de videojuegos actual. Pero, como decíamos en un principio, este portal no se limita a vender sus productos. En su página web suministran información sobre las próximas novedades, éxitos de ventas, en definitiva, todo lo que un aficionado a los videojuegos debe saber para mantenerse al día.

Esta tienda virtual ofrece a sus clientes la posibilidad de suscribirse con la finalidad de recibir información periódica acerca de actualizaciones, novedades y todo tipo de ofertas disponibles en su web. También incorpora una interesantísima sección desde la que es posible descargar múltiples fondos de escritorio con motivos tomados directamente de los videojuegos más populares. Y no sólo eso. También es posible acceder a *trailers* de los últimos lanzamientos cinematográficos y descargar vídeos de los videojuegos más esperados. Y para rematar, un *site* de lo más completo, dispondremos de multitud de enlaces a las páginas de las más importantes empresas de desarrollo, distribuidoras de software, etc. En definitiva, una tienda *on-line* más que interesante.

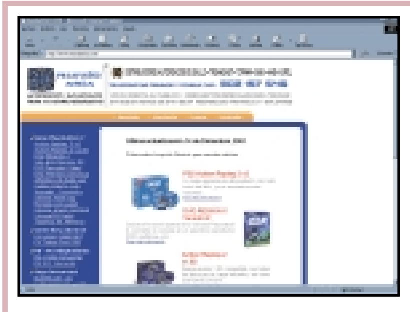



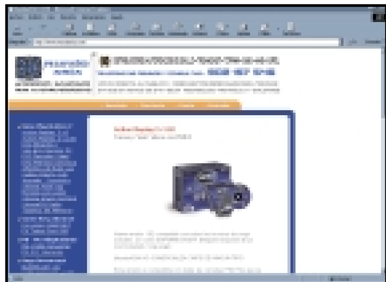
Movizonia

www.movizonia.com

Que la telefonía móvil ha conquistado nuestras vidas es de sobra conocido. Y además lo ha hecho en un tiempo récord. Como es lógico, Internet debía mostrar su particular apoyo a esta tecnología, y la mejor forma de hacerlo era prestando sus servicios para cobijar a una ingente cantidad de páginas dedicadas al mundo de la telefonía móvil. Y, precisamente, es en este ámbito donde destaca Movizonia. Este portal ha sido concebido como un completo bazar en el que es posible encontrar prácticamente cualquier dispositivo relacionado con esta rama de la telefonía. Desde los últimos teléfonos móviles GPRS hasta los accesorios más ingeniosos, todo tiene cabida en este completo portal. Pero esto no es todo lo que Movizonia ofrece a sus clientes. Los usuarios de esta página podrán enviar gratuitamente mensajes SMS, participar en foros en los que conversar con muchos otros usuarios de esta tecnología e incluso informarse sobre las últimas novedades leyendo completos artículos en los que se analizan de forma cuidadosa. En definitiva, una amplia gama de posibilidades que contribuye a incrementar el valor añadido de esta página y, en consecuencia, su interés.

El tan importante apartado de la seguridad ha sido contemplado para garantizar la privacidad de la información enviada por los clientes, de acuerdo con lo estipulado en la Ley Orgánica de Regulación del Tratamiento Autorizado de los Datos de Carácter Personal. Todo una garantía.





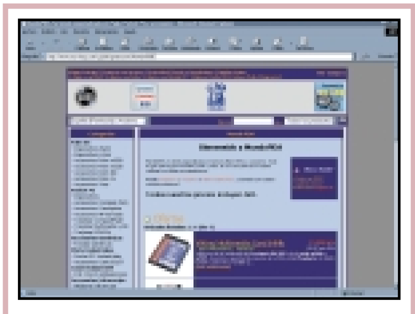
MundoASIA

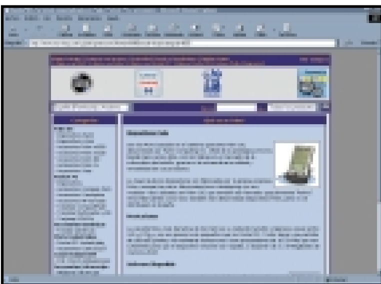
www.mundoasia.com

Este es uno de los portales dedicados al mundo de los videojuegos más curiosos. No porque en él se vendan las más novedosas consolas o los más modernos videojuegos. Estos dispositivos no los encontraremos en esta tienda virtual pero, a cambio, tendremos a nuestro alcance una enorme cantidad de accesorios, productos exclusivos realmente útiles destinados a ampliar la experiencia lúdica de los muchos aficionados a los videojuegos. Adaptadores, tarjeta de memoria, pistolas universales, mandos de control, mandos a distancia; en resumen, una amplísima variedad de accesorios, importados de los países orientales en la mayoría de los casos, que llenarán nuestro navegador de color y las mentes de los aficionados de ansia por probarlos.

El desplazamiento de los productos al domicilio de los clientes se efectuará a través de la agencia de transporte urgente SEUR, lo que garantiza que el usuario dispondrá de sus accesorios en un período de tiempo reducido. Para ofrecer a sus clientes el mejor servicio, MundoASIA acepta devoluciones de los productos siempre y cuando no hayan transcurrido más de siete días a partir de la fecha de recepción del pedido. Del mismo modo, y cumpliendo con lo estipulado por la LORTAD, otorga a sus clientes la posibilidad de eliminar de su base de datos toda aquella información que haga referencia a un cliente en particular, por supuesto, previa petición de éste.

Tras todo lo expuesto hasta este punto, debemos recomendar a los «adictos» a los videojuegos la visita de esta web, una de las más completas de su sector y, además, en perfecto castellano.





MundoPDA

www.mundopda.com

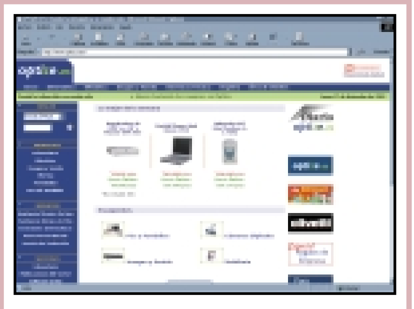
Son muchos los usuarios que día a día descubren el fascinante mundo de los asistentes personales digitales, también conocidos como PDAs. Estos pequeños e ingeniosos dispositivos sirven, sencillamente, para facilitarnos un poco la vida. Si aún no has descubierto estos adictivos y pequeños ordenadores, o si lo has hecho y has resultado atrapado por sus increíbles posibilidades, MundoPDA debe ser una página de visitada obligada.

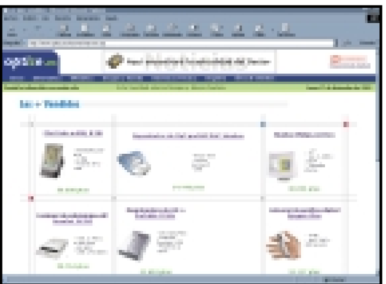
Esta completísima tienda virtual pone a disposición de todos los cibernautas una amplísima gama no sólo de PDAs, sino también de todo tipo de accesorios destinados a hacer de nuestra relación con estos pequeños compañeros de aventura una experiencia, si cabe, aún más placentera.

Con el objetivo de ofrecer a sus clientes un servicio inmejorable, MundoPDA añade multitud de servicios que contribuirán a acercar este universo a todos los públicos. Enlaces a páginas repletas de información sobre los Palm, vínculos a webs repletas de contenido dedicado íntegramente a la plataforma Pocket PC, en definitiva, una amplia variedad de opciones que contribuye a aumentar el valor añadido de una página ya de por sí tremendamente interesante.

Con la finalidad de garantizar la total privacidad de los datos de sus clientes, este interesante portal utiliza servidores con total soporte del protocolo SSL. Toda una garantía a tener muy en cuenta.

Tanto si lo tuyo son los PDAs como si te acercas por primera vez a este mundillo, MundoPDA es tu página. Imprescindible.





Optize

www.optize.com

Si te gusta la tecnología en general, esta es tu tienda virtual. En Optize encontrarás todo tipo de productos informáticos, de imagen y sonido y ofimática, integrando una de las más amplias ofertas a disposición de todos los usuarios hispanohablantes.

Pero Optize no es sólo una tienda, es un completo portal que brinda a sus usuarios la posibilidad de acceder a una gran cantidad de información relacionada con su área de negocio. Artículos sobre las evaluaciones que las principales revistas del sector hacen de este tipo de productos, glosarios de términos, una zona de descarga de software gratuito e incluso un diario en el que tienen cabida las principales noticias del sector, son tan sólo algunas de las muchas posibilidades de este *site*.

Su interfaz es enormemente atractiva, lo que unido a su sencillez de uso garantiza una agradable experiencia a todos sus usuarios. Localizar un producto es realmente sencillo, pudiendo hacerlo a través de los tan recurridos buscadores o utilizando los diversos escaparates que la web pone a disposición de todos sus clientes.

Las formas de pago entre las que pueden optar los clientes de esta tienda virtual son múltiples: pago con tarjeta de crédito, prepago, pago con ING Direct, fórmulas de financiación a particulares y a empresas, *leasing*, *renting* e incluso fórmulas a medida.

Por la variedad de los productos ofertados por esta compañía y la gran calidad de su servicio de venta, que contempla la devolución de productos y la garantía de obtener el mejor precio, Optize merece ser una de las tiendas virtuales de referencia en el segmento de productos informáticos y de imagen/sonido.



Utilidades para móviles

Servicios que la telefonía móvil e Internet ofrecen a los usuarios



En la actualidad ya podemos afirmar que la telefonía móvil se ha convertido en algo cotidiano prácticamente para cualquier persona. Esto se debe a que casi todo el mundo cuenta con teléfono móvil, ya sea para uso personal o profesional. Este enorme desarrollo se ha producido en gran parte debido a la amplia cobertura con la que contamos en la mayoría del territorio español y gracias a las subvenciones dadas a los fabricantes de terminales por parte de las operadoras. Esto último produjo un importante descenso en el coste de los teléfonos, por lo que casi cualquier persona podía tener acceso a un terminal de mayor o menor nivel por un precio muy asequible. Asimismo se produjo un descenso generalizado en el coste de las llamadas con la aparición de diferentes contratos.
Todo ello unido a la popularización de Internet ha provocado que el desarrollo de la tecnología de los teléfonos en sí haya comenzado a aumentar paulatinamente, ofreciendo cada vez una mayor gama de posibilidades. Por todo lo comentado, con un teléfono móvil podemos hacer muchas más cosas que comunicarnos por medio de la voz y eso es lo que vamos a ver a lo largo de este apéndice.

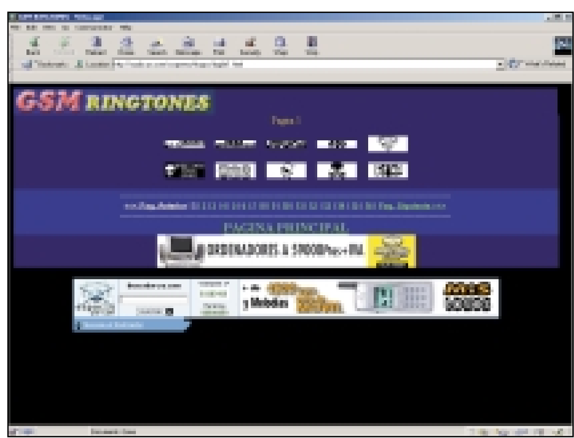
Mensajes de texto (SMS)

Uno de los servicios más utilizados, principalmente entre los usuarios más jóvenes de la telefonía móvil (entre 12 y 18 años), es el de los mensajes cortos o SMS, los cuales tienen un coste, dependiendo de la compañía y del tipo de contrato que tengamos, de entre 5 y 25 pesetas cada uno. La popularización de este tipo de mensajes ha sido la causa de la aparición de un nuevo argot en el que se emplean palabras que parecen auténticos jeroglíficos. Para que os hagáis una idea de lo extendido que está el uso de este servicio en nuestro país, os diremos que circulan alrededor de 8,5 millones de SMS diarios, y esta cifra va en aumento.
Sin embargo, cualquier persona que disponga de una conexión a Internet puede ahorrarse el coste de estos mensajes ya que es posible enviarlos a través de la Red. Esto se lleva a cabo por medio de algunas páginas específicas, aunque el número de caracteres en este caso disminuye con respecto a los habituales 120 que nos permite el propio terminal. Esto se debe a que por regla general estos *sites* de los que os hablamos suelen incluir su propia publicidad en cada SMS.
Contamos con un gran número de páginas disponibles en la Red, por poneros algunos ejemplos mencionaremos algunas de las más conocidas: *www.terra.es*, *www.navegalia.com*, *www.eresmas.com*, *www.amena.com*, *www.msn.es*, *www.movistar.com*, *www.airtel.es*, *www.excite.es*.

De todos modos, y con el objetivo de ahorrar caracteres a la hora de enviar un mensaje de texto, en nuestro país se están estandarizando oficiosamente una serie de abreviaturas que se utilizan en estos entornos. Así se logra decir más cosas en un mismo mensaje y de este modo ahorrarse costes. Precisamente por ello es tan útil el servicio que no ofrece Internet, ya que por el mismo precio podremos enviar todos los mensajes que deseemos. A continuación os mostraremos algunas de las abreviaturas más comunes:
— La *h* y la *e* al principio de las palabras desaparecen.
- Se sustituye *ll* por *y*, *porque* por *xq*, *para* por *xa*, *pero* por *xo*, *también* por *tb*, *todavía* por *td* o *mañana* por *mn*.
— Se utilizan signos matemáticos: *más* se puede cambiar por + o *menos* por -.
— En muchas expresiones se utilizan tan sólo las iniciales: *te quiero* es lo mismo que *tq*, *bd* es *buenos dias* o *hasta luego* es *hl*.
— Se aprovecha el sonido de las consonantes: *te (t)*, *k (ca)*, etc.

Mensajes con imágenes

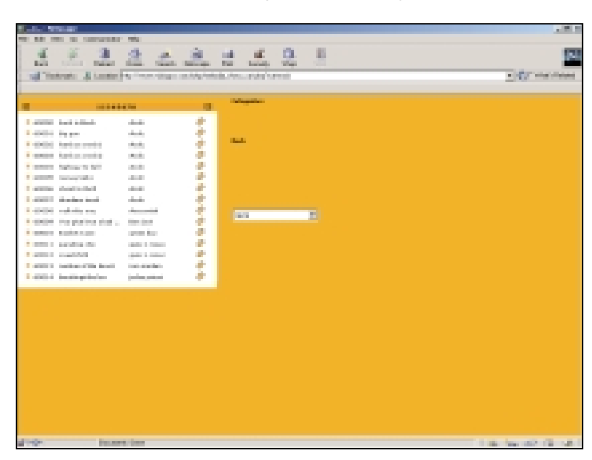
Muchos terminales también nos ofrecen la posibilidad de enviar y recibir imágenes. Éstas suelen venir predefinidas y almacenadas en el mismo teléfono, por lo que podremos usarlas al instante, pero también tenemos la posibilidad de poder descargarlas de Internet por un pequeño coste en algunos casos, gratuitamente en otros. Encontramos imágenes de diferentes motivos: amor, felicitaciones, saludos, etc. Pero claro, esta alternativa tiene un problema, y es que el coste de enviar una imagen es aproximadamente el mismo que el de cuatro mensajes de texto convencionales. Éstas las podemos encontrar en multitud de páginas, de todos modos hay que tener en cuenta que generalmente las webs de las operadoras o de los propios terminales que tengan soporte para ello por regla general suelen tener esta posibilidad.
Algo muy similar ocurre con las melodías, hablamos de la

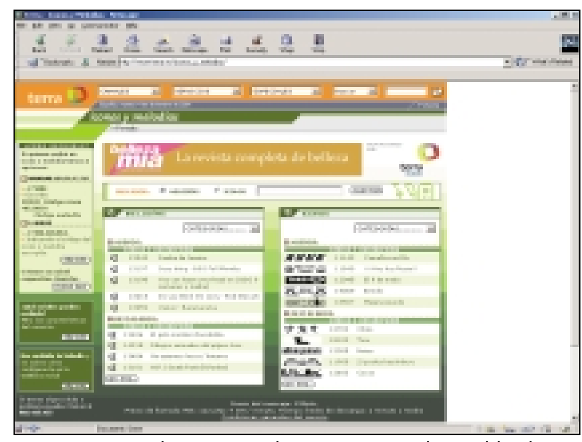


posibilidad que estos usuarios tienen de componer sus propias canciones por medio de un compositor que suelen incluir los propios terminales. No obstante, también podremos descargar dichas melodias de la Web o incluso componerlas con algún software específico que se encuentre en la propia página.

WAP

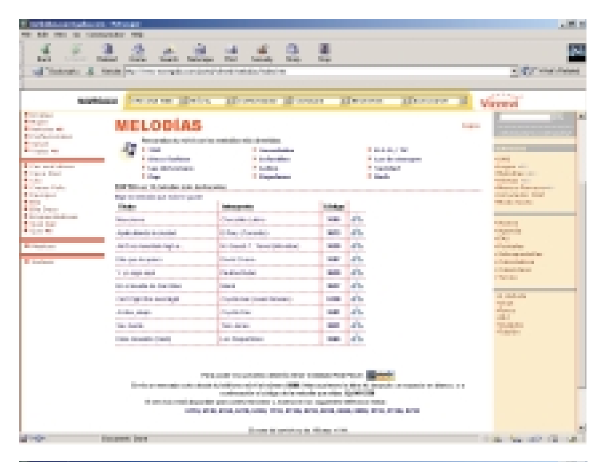
Este es uno de los servicios que ya se han convertido en habituales en la telefonía móvil actual. De hecho, la mayoría de modelos de gama media/alta que se están lanzando al mercado ya cuentan con este soporte. WAP son las siglas de *Wireless Aplication Protocol* o Protocolo de Aplicaciones Móviles, y para que os podáis hacer una idea aproximada de lo que esto significa, os diremos que se trata de un protocolo mediante el cual es posible la conexión a contenidos de Internet desde un terminal móvil. Está basado en el modelo web de Internet, aunque viene condicionado por la velocidad de acceso y por la interfaz del usuario, o mejor dicho, del terminal de conexión. Esto se debe principalmente a que la pantalla que nos ofrecen los teléfonos móviles actuales no tienen nada que ver con un monitor de ordenador, de forma que lo que el usuario ve hay que acoplarlo a ese pequeño LCD.
En su afán de imitar el sistema de Internet, WAP cuenta con su propio lenguaje de comunicación específico conocido como WML (además del complemento WMLScript), aunque utiliza la misma red GSM, o en su defecto GPRS, que usamos para la voz. WAP es un protocolo que permite acceder desde el móvil a gran cantidad de servicios de Internet. Nos referimos, por poner algunos ejemplos, a correo electrónico, navegación Web o chat. Aunque estos servicios resultan sumamente atractivos para el usuario, también es cierto que no han cuajado como los fabricantes y operadoras esperaban, ya que no ha tenido demasiado éxito. Esto se debe principalmente a la corta velocidad de conexión que desde un teléfono móvil podemos lograr, ya que es de tan sólo 9.600 bps, un valor demasiado escaso si queremos navegar por la Web, más si tenemos en cuenta que en algunos casos tenemos que descargar imágenes, por ejemplo.
Además de esto, el poco éxito de WAP también viene dado porque los servicios ofrecidos no se basaban en una plataforma común. Para solucionar este inconveniente, la Asociación GSM formada por las principales operadoras de telefonía móvil anunció antes del verano la iniciativa *M-Services*, cuya finalidad es que los usuarios cuenten con una plataforma común para navegar por Internet desde su móvil. De hecho, la compañía Openwave ya ha lanzado, apoyando esta iniciativa, su nuevo *Micronavegador* acompañado del software de descarga *Download Fun*. La principal característica de este novedoso navegador, cuya versión WAP ya está integrada en el Siemens SL-45, es que se reducen los pasos para encontrar una información en concreto. Todo ello debido a los menús emergentes o los campos extensibles y la navegación se hace más amena gracias a la inclusión del color y de las imágenes. También podremos descargar archivos fácilmente tales como melodías o logos para el móvil (de lo que ya os hemos hablado).
Debido a iniciativas como esta y a la reciente inclusión de los servicios GPRS, esperamos que el uso de algo tan útil como



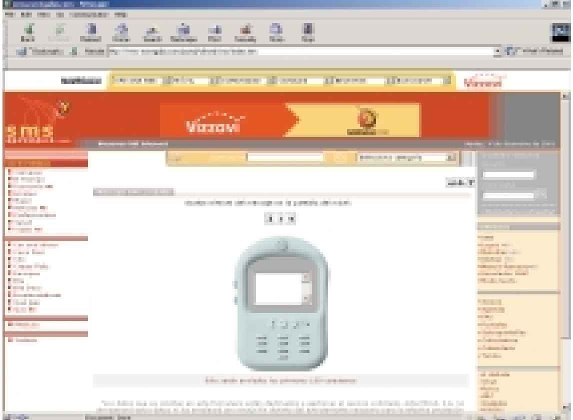


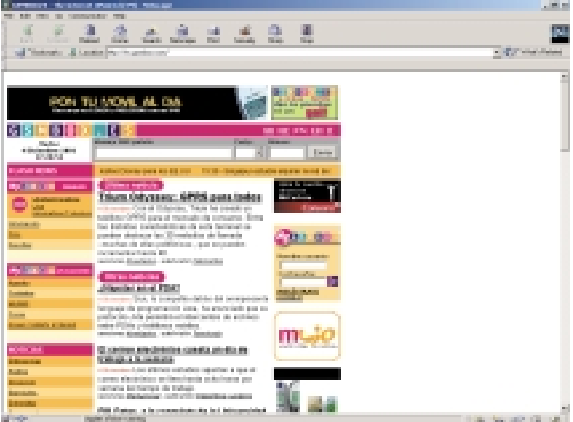
Iconos, logos y melodías en Internet

Estas son algunas de las direcciones en las que podréis encontrar recursos para animar vuestro móvil con divertidos logos o melodías.
http://es.gsmbox.com/
www.sumovil.com/
www.nokia.es
http://es.telelogo.net/logos/
www.tuslogos.com/
www.laplazamenor.com/logos.htm
www.vj2000.org/logosm.shtml
http://vendaval.htmlplanet.com/logos.html
www.es.fm/logos/
http://todomoviles.miarroba.com/
www.cellnews.net/archivo/Melodiasteclas.htm
http://logos.chatmix.net/
www.movilonline.com/
www.akimusica.com/ringtones.cfm
www.maximovil.com/ringtones/default.asp
http://members.es.tripod.de/o_mas/grupos/magodeoz/moviles.htm









el protocolo WAP comience a mejorar y de este modo a instaurarse de forma definitiva en el mercado de la telefonía móvil. Bien es cierto, por otro lado, que aún queda mucho camino por recorrer para que la conexión a Internet a través de un terminal móvil sea algo común para cualquier usuario.

Futuros servicios WAP

Para lograr el objetivo de extender más los servicios que nos ofrece este protocolo de comunicaciones, algunas empresas están desarrollando diversos proyectos, de los cuales daremos algunos ejemplos a continuación.

Tripod es una comunidad *on-line* del portal Lycos que entre otras cosas ofrece herramientas para la creación de páginas web para todo tipo de usuarios, desde los principiantes en programación HTML, hasta los expertos en este tipo de código. Además, recientemente ha incorporado un servicio que ofrece la posibilidad de que los propios usuarios creen páginas para móviles WAP, con un procedimiento igual de sencillo que el que se sigue para crear una página web y con la posibilidad de registrar los *sites* en los principales buscadores de Internet. Sus usuarios pueden beneficiarse de los servicios de Lycos, como un correo electrónico gratuito con 15 Mbytes de espacio. De momento, todos estos servicios son gratis, pero en breve va a existir una versión de pago denominada Premium. Con ella se dispondrá de



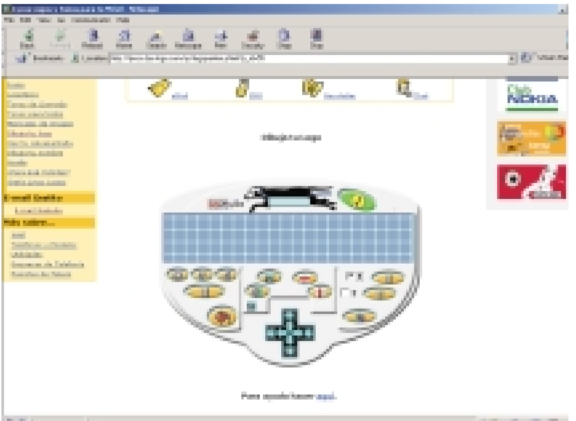
hosting de páginas, de cuentas de correo, de estadísticas de tráfico, así como de la posibilidad de registro de dominios.

Por otro lado, e-mocion, plataforma de acceso a contenidos WAP de Movistar, ofrece una gran cantidad de servicios informativos a los usuarios de la propia operadora. Además recientemente acaba de lanzar uno nuevo para escuchar música *on-line* desde el móvil. Esto se ha logrado gracias a un acuerdo alcanzado con la compañía Musiwap, líder en Europa como proveedor de contenidos de música para las operadoras de telefonía móvil. Para utilizar este servicio tan sólo hay que entrar en el menú *Música* de e-moción y seleccionar las opciones correspondientes. En un principio tan sólo sirve para encontrar información sobre canciones. Sin embargo, en un corto plazo de tiempo se permitirá a los usuarios de e-moción escuchar la música elegida desde su teléfono móvil.

Música en el móvil

Al igual que la telefonía móvil ha ido ganando cada vez más adeptos, otra tecnología que se ha extendido de manera muy rápida ha sido la de los reproductores MP3. Al tratarse de dos tecnologías móviles, algunos fabricantes han optado por fusionarlas en algunos casos. De este modo, ya sea por medio de un adaptador especial (como en algunos modelos de los fabricantes Nokia o Ericsson) o incluido en la circuitería del propio terminal (Siemens SL-45), podremos disfrutar de música en este formato en el mismo teléfono. Para poder escuchar este formato de música en nuestro terminal móvil resulta imprescindible el hecho de que anteriormente nos bajemos los temas desde Internet. Esto es algo que podemos llevar a cabo por medio de alguno de los múltiples *sites* que podemos encontrar en Internet para estas labores.





Posteriormente bastará con que las carguemos en el móvil y disfrutar de ellas.

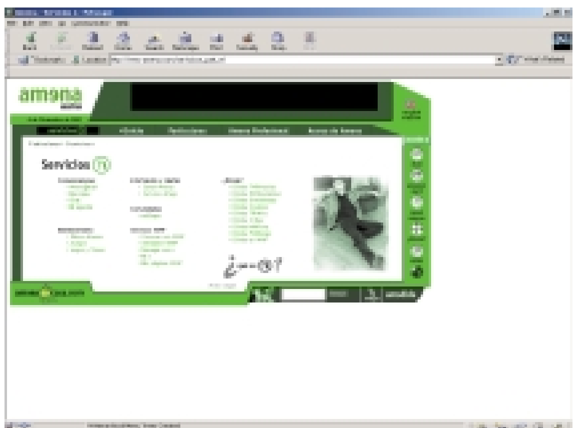
Pago a través del móvil

Quizá una de las utilidades más curiosas que un teléfono móvil nos puede ofrecer hoy en día es aquella que se conoce como *Pago con móvil*, con la que nuestro terminal puede convertirse en algo similar a una tarjeta de débito. Existen algunas páginas en Internet como es *www.paybox.es* que ofrecen este servicio y cuya utilización es extremadamente sencilla. Para empezar diremos que todas las operaciones monetarias se realizan por medio de la red GSM, y no por la de Internet, por lo que se gana en seguridad. Sin embargo, para poder darnos de alta y contratar el servicio resulta imprescindible hacerlo a través de la web. Asimismo debemos tener en cuenta que es compatible con cualquier operadora de telefonía móvil, y que podemos trabajar con cualquier entidad bancaria.
Para utilizar paybox basta con hacer una llamada, y tendremos a nuestra disposición una serie de servicios: enviar dinero a cualquier número de móvil o cuenta bancaria, recibir dinero directamente en nuestra cuenta bancaria o pagar bien en Internet o en tiendas. Una vez nos hemos registrado y dado de alta en el servicio por medio de la página que os hemos comentado, todo se realiza a través de SMS y pagamos en las tiendas dando un código que nos envía el servicio y que debe confirmar el comerciante para que acepte el pago y éste se nos cargue en la cuenta.

GPRS y UMTS

Todos los servicios y utilidades que Internet es capaz de ofrecernos se verán enormemente incrementadas con la consolidación de la tecnología GPRS y la futura implantación de UMTS.





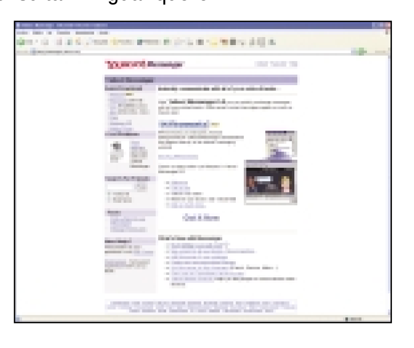
GPRS (*General Packet Radio Service*) ofrece diferentes ventajas con respecto a GSM; por poner algunos ejemplos, mencionaremos que GPRS permite que el usuario pague tan sólo por la información que transmite, no por el tiempo de conexión, ya que esto último no consume recursos de la red a la que estemos conectados. Del mismo modo el coste por establecimiento de llamada es nulo. Esta es una tecnología que, al estar especialmente diseñada para la transmisión de datos, precisa de un mayor ancho de banda que su predecesora. Es por ello que GPRS permite que el usuario tenga, si así lo desea, asignados varios canales de datos, por lo que el ancho de banda disponible está directamente relacionado con el número de canales que utilicemos simultáneamente, aunque también el coste, por supuesto. Para que os podáis hacer una idea de lo que esta tecnología es capaz de ofrecernos a la hora de bajar datos de Internet a nuestro teléfono móvil, cabe destacar que hasta el momento la velocidad estimada del WAP es de 9,6 Kbps, sin embargo GPRS permite una velocidad de transmisión máxima estimada de 171,2 Kbps, aunque en la realidad esta cifra desciende hasta los 20 o 30 Kbps de media.
En cuanto a UMTS, cuyas siglas responden a *Universal Mobile Telecommunications System*, todavía tendremos que esperar a su implantación. Es cierto que ya hay fabricantes que disponen de prototipos que utilizan esta tecnología, pero no habrá terminales funcionando hasta dentro de varios años. El éxito esperado vendrá gracias a sus supuestos 384 Kbps de velocidad de transferencia media y a los 2 Mbps de velocidad punta máxima que ofrece UMTS, por lo que se pretende que desde un terminal de este tipo tengamos la posibilidad de realizar infinidad de tareas, incluso videoconferencia, aunque esto suene a ciencia-ficción.



Mensajería instantánea

ICQ y Yahoo! Messenger / CD

Al llegar el correo electrónico supuso una revolución al ser, con diferencia, mucho más rápido que el correo convencional. Pero como todo evoluciona, muchos deseábamos una alternativa de comunicación más rápida. De ahí surgió la mensajería instantánea, con la que podemos comunicarnos en tiempo real con la persona que deseemos. Es una herramienta utilísima para establecer comunicación con nuestros amigos y familiares y que, a pesar de carecer de la formalidad del correo electrónico, se usa cada vez más como herramienta dentro de las empresas para facilitar el intercambio de información entre sus empleados sin tener que desplazarse o mandar un *e-mail* para una simple consulta. Al igual que el correo electrónico, puede enviar archivos de todo tipo y además tiene la posibilidad de establecer conferencias de vídeo, realizar charlas con voz e incluso de comunicarnos, a la vez, con el número de personas que deseemos invitar a una charla.



La mensajería instantánea está llena de posibilidades y lo mejor de todo es que está en plena expansión y cada día ofrece muchos más servicios para el usuario. Los grandes líderes dentro de este tipo de programas son ICQ, Yahoo! Messenger, Windows Messenger y AOL Instant Messenger. La mayoría de ellos ofrecen las mismas posibilidades, ya que hay una rivalidad latente entre estos productos y, cuando alguno ofrece una función nueva, rápidamente sale al mercado una versión posterior de los demás con esta misma función mejorada. Hay una gran competencia por ser el número uno y los más beneficiados de esto somos los usuarios, puesto que el producto se mejora día a día. Lo mejor de todo es que son programas gratuitos, sólo es necesario registrarse para obtener un nombre de usuario y una contraseña. A partir de ese momento ya estaremos listos para entrar a formar parte del mundo de la mensajería instantánea. Podemos utilizarlo de forma lúdica, bien sea para hacer amigos por la red o charlar con nuestros amigos o incluso para facilitarnos nuestra comunicación en el trabajo. A continuación desmenuzamos dos de los más populares, por funcionalidad y número de usuarios: ICQ y Yahoo!Messenger.

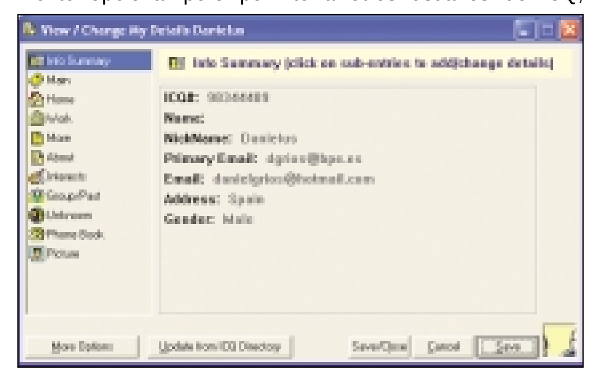
ICQ www.icq.com

I seek you es el curioso origen de este nombre. Leído en inglés, es prácticamente idéntico a pronunciar las siglas mágicas: «I», «C», «Q». En definitiva, es una revolucionaria herramienta para Internet que nos informa de quién está en línea en cualquier momento y nos permite contactar con una persona. Ya no es necesario buscar en vano en Internet a amigos o compañeros. ICQ hace esta búsqueda por nosotros, alertándonos en tiempo real cuando se conectan nuestros conocidos. Podremos también chatear, enviar mensajes, ficheros, direcciones, jugar o simplemente saber quién se encuentra en línea cada momento. También nos permite elegir el modo de comunicación que deseemos emplear en cada momento. Independientemente de la aplicación, ya sea chat, voz, conferencia, transferencia de ficheros o juegos por Internet. ICQ soporta una gran variedad de aplicaciones muy populares de la Red y sirve como una plataforma universal desde la cual lanzar cualquier aplicación «punto a punto» como Microsoft NetMeeting o Netscape CoolTalk. También puede ser usado en un modo multiusuario, de tal forma que un grupo puede organizar una conferencia o simplemente «pasar el rato» en línea. El programa se ejecuta en segundo plano, apropiándose de una porción mínima de memoria y recursos de red. Mientras que trabajamos con otras aplicaciones, ICQ nos alerta cuando nuestros amigos o conocidos se conectan, permitiéndonos trabajar eficientemente mientras que se mantiene un amplio rango de funciones de Internet. Entre las funciones disponibles se encuentra: chat, mensajes, correo electrónico, URLs y transferencias de ficheros. Dos son las grandes novedades de la última versión: en primer lugar, la lista de contactos se guarda en el servidor, por lo que podemos cambiar de PC sin tener que dar de alta de nuevo a nuestros amigos; y la segunda es que existe una versión denominada *ICQ Lite* a la que se accede a través de *www.icq.com* y que nos permite usar ICQ sin tenerlo instalado. A pesar de disponer sólo de las funciones más básicas, esto nos permitirá usar ICQ en cualquier cibercafé o universidad, sin necesidad de bajar e instalar el programa.



Cómo funciona

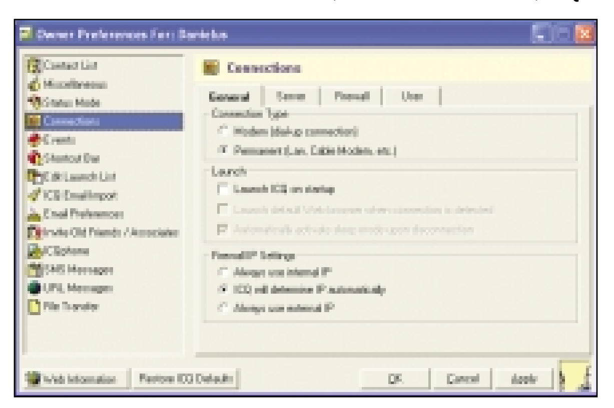
Es fácil. Cuando instalamos ICQ, el programa nos pide que nos registremos en un servidor, que está a su vez conectado a una vasta red de servidores extendidos por Internet. Durante la instalación, recibimos un número de ICQ único, también conocido como UIN (*Universal Internet Number* o Número Universal de Internet). Además, ICQ nos da la opción de introducir información personal a la vez que el número. Esto es totalmente opcional pero permite a otros usuarios de ICQ,



reconocernos cuando nos conectamos y establecer gustos y aficiones comunes. Una vez registrados, podemos formar una lista de amigos y compañeros de varias formas. ICQ usa esta lista para encontrarlos por nosotros. Mientras tanto, ICQ permanece en segundo plano sin interrumpir a las demás aplicaciones en uso. Tan pronto como nos conectemos a Internet, automáticamente detecta nuestra conexión, anuncia nuestra presencia a la comunidad de usuarios en la Red (si así lo deseamos) y nos informa de la presencia de contactos en línea. Una vez que sabemos quién está «ahí», todo lo que queda por hacer es hacer clic en un icono para comenzar a chatear, transferir información o ficheros, enviar mensajes, intercambiar archivos o lanzar cualquier aplicación externa «punto a punto».

Conexión

Después de la instalación, ICQ se ejecuta automáticamente. Si no lo hace, debemos hacer doble clic en la flor que ha aparecido en nuestro escritorio. Si ya somos un usuario registrado en ICQ, debemos seleccionar *Existing User* e introducir correctamente nuestro número de ICQ y contraseña. Por defecto, esta utilidad empieza automáticamente en cuanto nos conectamos a Internet. Si queremos evitar esto, sólo tenemos que dirigirnos a *Main/Preferentes/Connection* y deseleccionar *Launch On Startup*. Si por el contrario disponemos de una conexión permanente tipo ADSL o red, debemos acceder al mismo sitio y seleccionar *Permanent*. Finalmente, si usamos un *firewall*, ICQ



intentará detectar la configuración del mismo de forma automática. En caso de que no sea así, siempre podremos configurarlo manualmente en *Main/Preferentes/Connection/Firewall*.

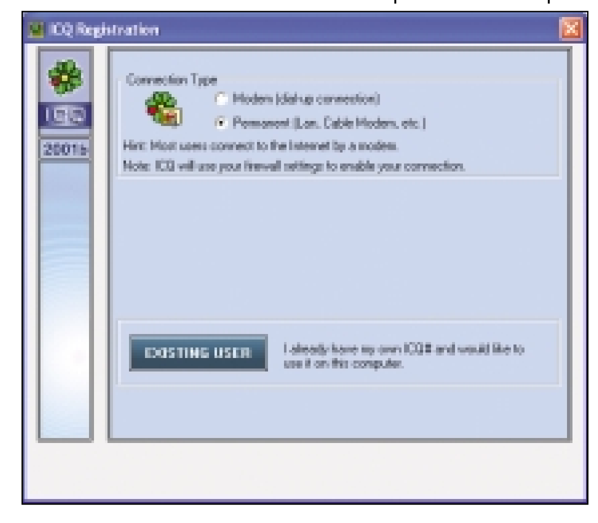
Preliminares

Los botones *Services*, *My ICQ* y *Main/ICQ* están localizados en la parte baja de la ventana principal. El botón *Main/ICQ* cambia la apariencia entre los dos cuando situamos encima el puntero del ratón. Los tres botones son el centro de control para ICQ. Justo encima se encuentra la lista de contactos donde está la gente que hemos añadido anteriormente al programa. ¿Qué hacemos si está vacía? El nuevo ICQ2001b ofrece una manera fácil de encontrar amigos y otras personas que compartan nuestros gustos e intereses. En la parte superior, hacemos clic en *Find a Friend*. Esto hará una búsqueda por todos los servidores de ICQ en busca de usuarios compatibles. Además, podemos pulsar sobre *Add/Invite Users* para localizar a nuestros amigos y compañeros. Una vez que tengamos un contacto en línea, tan sólo haremos doble clic encima para que aparezca una ventana de texto donde nos pondremos comunicar. Por otro lado, hay dos indicadores de status en ICQ. Uno indica el status de nuestros contactos y el otro el nuestro propio. El de nuestros contactos se encuentra a la izquierda de cada nombre. El nuestro está situado abajo a la derecha. Es el famoso icono en forma de margarita que de color verde indica *on-line* y de color rojo *off-line*.



Calentando motores

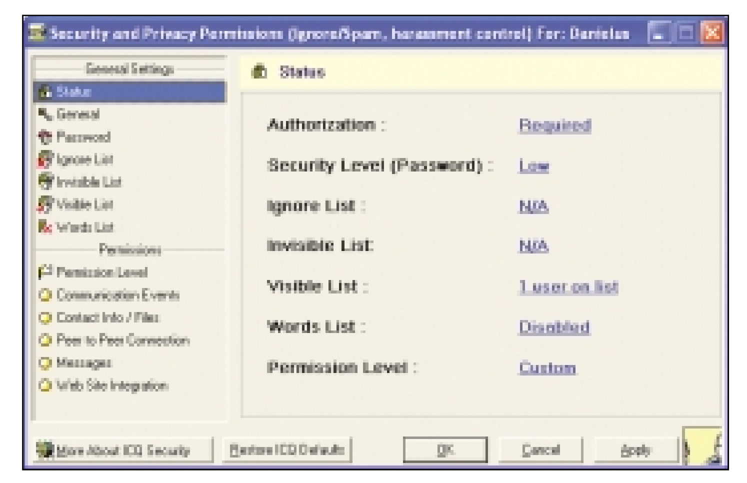
Una gran ventaja de este programa es la posibilidad de usar más de un número ICQ en el mismo PC. Para ello debemos ir a *My ICQ* y seleccionar *Registration to ICQ*. Luego, *Register a New User*. Después, para cambiar entre un número y otro debemos ir a *My ICQ* y elegir *Change User On This Computer*, para luego seleccionar *Add Another Registered User*. Hay dos modos en ICQ, avanzado y simple. *Advanced Mode* permite acceder a todas las funciones. Es ideal para usuarios experi-



mentados. Sin embargo, si somos novatos, lo ideal es comenzar con *Simple Mode*. Para cambiar entre uno y otro debemos ir a *Main/Advanced Mode* y viceversa. Pero, ¿cómo podemos enviar una petición de chat a un contacto? Tan sólo tenemos que hacer clic con el botón derecho sobre él y seleccionar *ICQ Chat*. Una vez que el otro lado haya aceptado la petición, se producirá la conexión entre ambos. Así como las sesiones de *chat* se pueden guardar, también tenemos el *Message Archive* que se encuentra en *My ICQ* y que es un archivo donde se van almacenando todas nuestras conversaciones. Es totalmente configurable y podremos acceder a él, evitar su uso, borrar parte, etc.

Opciones avanzadas

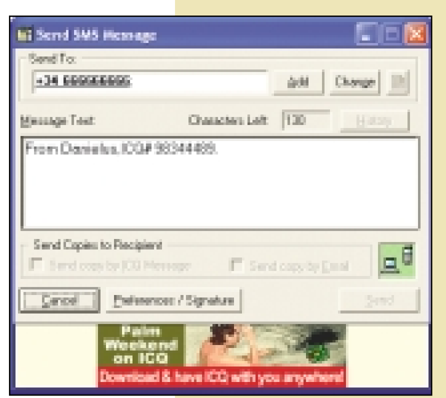
Podemos dividir a nuestros contactos en grupos diferentes. Esto nos permite gestionar los mensajes de forma más eficiente. Tenemos la posibilidad de enviar mensajes a un grupo entero o a unos determinados miembros. Para cambiar a este *Group Mode*, hay un botón en la ventana principal denominado *Contact List Groups*. Además, los grupos son totalmente configurables, pudiendo añadir o eliminar contactos sin limitaciones. Para mandar un mensaje a un grupo, tenemos que hacer clic en el grupo y elegir *Send Message To* y seleccionamos *Entire Group*. Por otro lado, cuando nos registramos, lo



hacemos dando una serie de detalles sobre nosotros. Si queremos cambiar esos datos, nos dirigimos a *Main/View Change My Details*. Si por cualquier motivo un día nos encontramos con otra persona con nuestro mismo nombre no debemos asustarnos, esto es totalmente normal. Lo que diferencia a un usuario de otro es el número de ICQ no el nombre. Para una personalización total, podemos añadir incluso una foto nuestra. En el tema de seguridad y privacidad, si no queremos que cualquier persona pueda añadirnos a su lista de contactos, debemos ir a *Main/ICQ/Security & Privacy Permissions/General* y seleccionar *My authorization is required befote users add me to their contact list*. En un caso extremo, siempre podemos eliminar nuestro número de ICQ para no dejar rastro. Para ello debemos ir a *My ICQ/Registration to ICQ/Un-register Existing User*. Sin embargo, es importante recordar que, aunque añadamos a alguien a nuestra lista de contactos, no nos verá hasta que nos añada también por su parte.
Otro aspecto importante son los modos de estado. Hay algunos automáticos como «ocupado», «no disponible» u «offline», aunque podemos definirlos en cualquier momento haciendo clic en la flor. Finalmente, si queremos deshacernos de algún «pesado», podemos añadirle a nuestra lista de usuario ignorados en *Main/Security & Privacy Permissions/Ignore List*.

Ficheros, SMS, e-mail y teléfono en ICQ

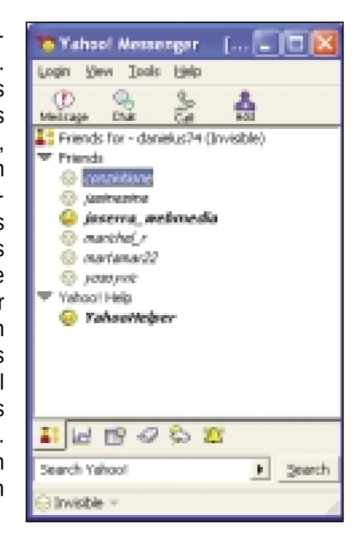
Todas estas funciones son de tipo «punto a punto» por lo que a veces obtendremos un mensaje de error del estilo de *Can't Establish Direct Connection*. Hay muchas razones para esto pero la más común es que alguna de las dos partes tenga un *Firewall*. De todas formas, si sólo una de las partes está afectada por esto, muchas funcionalidades se podrán llevar a cabo de un lado al otro aunque no al revés. Por otro lado, una de las grandes ventajas que tiene el envío de ficheros a través de ICQ es que no hay límite en el tamaño. Además, si por cualquier razón una transferencia se queda atascada en algún punto, podemos comenzar de nuevo y probar a poner la barra de velocidad por la mitad. En cuanto al servicio de SMS, podremos mandar mensajes a teléfonos móviles de todo el mundo usando los servidores de ICQ. Aunque no todos los operadores de telefonía móvil están soportados, hay una larga lista de ellos. Lo mejor es hacer una prueba para comprobar si funciona. No solamente es un servicio gratuito sino que no lleva publicidad, por lo que disponemos de los 160 caracteres, cosa que no ocurre con los servicios similares que se extienden por la Red. Por otra parte, contamos con la interesante posibilidad de que la persona que reciba el SMS conteste directamente al mismo y el mensaje de respuesta nos llegará a nosotros al mismo ICQ como un mensaje de texto corriente. En otro orden de cosas, también podremos hacer llamadas gratuitas PC a PC con ICQ y su cliente de telefonía incorporado. Tan sólo necesitamos una tarjeta de sonido, altavoces y micrófono. Si lo que queremos es llamar a un teléfono convencional, o sea, una comunicación PC a teléfono, si tendremos que pagar algo, pero el precio es muchísimo menor que si llamáramos desde un teléfono particular. Para finalizar, conviene recordar que con ICQ podemos no sólo consultar nuestra propia cuenta de correo tipo POP sino que también tenemos la posibilidad de tener una cuenta tipo Web de ICQ.



Yahoo! Messenger http://messenger.yahoo.com

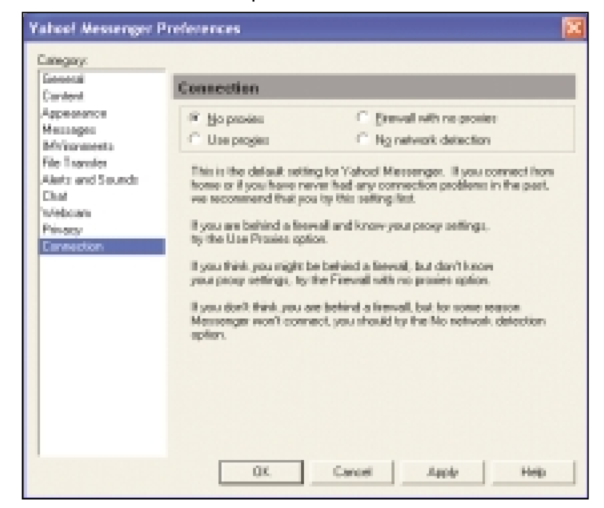
En primer lugar, necesitamos una cuenta Yahoo!, cualquier versión de Windows y Microsoft Internet Explorer 4.01 o superior. Opcionalmente, un micrófono y altavoces (para usar las llamadas por voz) y una *webcam* para el vídeo en tiempo real. Con respecto al Yahoo! ID, nos aparecerá un cuadro de diálogo que nos pedirá un nombre de usuario. Si no tenemos, debemos hacer clic en *Get a Yahoo! ID*. Lo primero que nos aparece es una serie de campos con nuestro nombre y datos personales. Luego, se nos sugiere una serie de IDs aunque

podremos confeccionar uno personalizado asociado a una palabra clave. Cada ID en Yahoo! Messenger es único, de forma que puede resultarnos difícil encontrar uno libre. Por último, hemos de poner una combinación pregunta – respuesta que nos será formulada en el caso de que olvidemos nuestra palabra clave. No debemos olvidar que este identificador no se puede cambiar y tendremos que crear uno nuevo si queremos hacerlo. Sin embargo, podemos tener cuantos «alias» queramos. También, durante el proceso de instalación, deberemos elegir instalar o no varias aplicaciones. Una de ellas es *Yahoo! Companion*, un conjunto de utilidades que se integran con nuestro navegador de Internet.



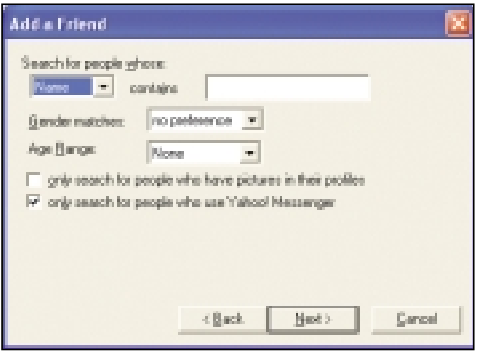
Conexión

Lo primero que se nos pide al ejecutar la aplicación es nuestro ID y contraseña. Si compartimos nuestro PC y no queremos que todo el mundo pueda acceder a nuestra cuenta, debemos asegurarnos que la casilla *Remember my ID & Password* no esté seleccionada. La forma de saber si estamos conectados es fijándonos en la lista de amigos. Cuando aparezca y veamos quiénes están o no conectados, estaremos en línea. Si tenemos problemas o si se nos cae constantemente la conexión, será debido posiblemente a un *firewall*. Para configurarlo debemos ir al menú *Login* y seleccionar *Preferences* y *Connection*. Las opciones de *proxy* son para usuarios que están detrás de un SOCKS y/o un *proxy* HTTP. Si estamos intentando conectarnos a través de un *firewall* que no usa un servidor *proxy*, Yahoo! Messenger buscará automáticamente el *firewall* y ,si lo llega a encontrar, lo usará para conectarse. Si no lo consigue, tendremos que habilitar el puerto 5050 para los servidores predeterminados de Yahoo! Messenger. Si por el contrario tenemos un *proxy* HTTP, deberemos habilitar la casilla correspondiente en la pantalla de configuración. Si salimos a Internet a través de un *router* que no permite otra cosa que no sea llamadas HTTP, entonces debemos seleccionar la casilla *Firewall with no proxies*. En esta línea, una opción muy interesante es el modo invisible. Significa que podremos ver sin ser vistos. A pesar de esto, cabe la posibilidad de enviar y recibir mensajes, aunque a nuestros amigos les seguiremos apareciendo como *off-line*. Para arrancar siempre con este modo, debemos ir al menú *Login/Change User/Login under Invisible Mode*. Si estamos conectados de otra forma y queremos cambiar a este modo, lo podremos hacer en *Login/Change My Status/Invisible Mode*. Si nuestros amigos aparecen en la lista con letra cursiva, esto significará que estamos en modo invisible.



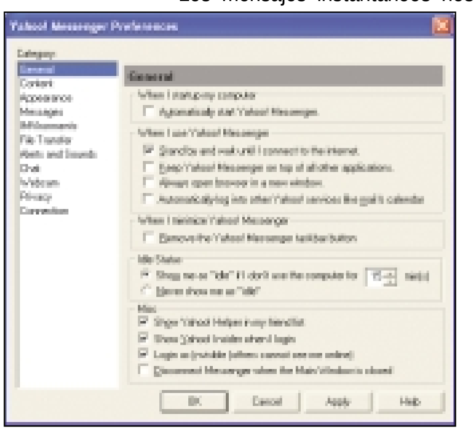
Lista de amigos

Para añadir amigos, abrimos el programa y hacemos clic en el botón *Add*. Aparecerá una nueva ventana donde se nos pedirá su ID. Si no lo conocemos, siempre podemos hacer una búsqueda en *Tools/Manage Friend List/Search for a Friend*, donde tendremos varias posibilidades: palabra clave, nombre, ID, etc. Lo siguiente será elegir el nombre del grupo donde lo queramos colocar. También podremos elegir si usar nuestro ID o un alias para añadir a nuestro amigo. Este sólo verá el alias que nosotros queramos que puede ser diferente del resto. Por último, la próxima vez que nuestro contacto se conecte, tendrá la opción de aceptar nuestra invitación o rechazarla. Todo esto nos será convenientemente notificado mediante mensajes. Para borrar un contacto de la lista, sólo tendremos que hacer clic con el botón derecho encima de él y seleccionar *Delete*. Si hacemos esto, nuestros contactos no recibirán un mensaje de información. A pesar de hacer esto, podemos seguir mandando mensajes a través del botón *Send*, introduciendo su ID. Si por el contrario tan sólo queremos no recibir más mensajes de una persona, podemos ignorarle haciendo clic en el botón *Ignore User*. En otro orden de cosas, si queremos hablar con varios amigos a la vez (hasta 10), podemos invitarlos a una conferencia. Esto lo llevaremos a cabo de dos maneras. Una en *Tools/Invite to Conference* y otra en *Friend/Invite to conference*. Si todo va bien, se abrirá una nueva ventana en donde se realizará la charla y veremos en la parte izquierda los contactos participantes. También, en *Tools/Manage Friend List* podemos crear, organizar y configurar un grupo.



Mensajes

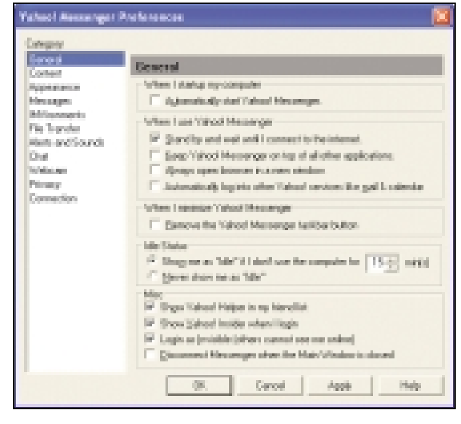
Los mensajes instantáneos nos permiten comunicarnos con nuestros amigos en tiempo casi real. Son muy similares a un correo electrónico, pero con la diferencia de que no tenemos que esperar horas a una respuesta. Podemos incluso salvar en un fichero de texto nuestra conversación entera con un amigo. Sólo tenemos que ir a *File/Save*. Se puede realizar esta operación con todas y cada una de las conversaciones para mantener un historial. Los pasos a seguir son: *Login/Preferences/Messages/Enable Archi-*



ving. Si en un determinado momento queremos consultar este historial, debemos ir a *Tools/Message Archive*. A nivel estético, podemos incluso cambiar la fuente y el color del texto que escribimos. Además, tendremos la posibilidad de usar una de las opciones más valoradas y queridas por los usuarios de esta utilidad. Estamos hablando de los *smileys*. Son unos pequeños iconos muy graciosos que nos permiten expresar emociones como miedo, sorpresa, alegría, duda, etc. En la propia ventana donde se escribe el texto hay una lista desplegable con un montón de ellos. Si somos usuarios avanzados, podemos escribir directamente el atajo de teclado correspondiente que aparece en la ayuda. Por otra parte, para enviar un mensaje a un contacto en particular, primero debemos asegurarnos de que esté en línea y luego hacemos doble clic sobre él, para luego aparecernos una ventana de texto donde empezaremos la comunicación. Hay que observar que no tenemos por qué dejar por defecto el ID de un contacto, ya que si hacemos clic con el botón derecho del ratón, podremos darle a cada persona el nombre que nosotros queramos, independientemente de su ID. Otra opción consiste en mandar un mensaje a varios destinatarios. Para ello debemos seleccionar *Message* en la barra de herramientas y en el campo *Yahoo! ID* metemos el nombre de los contactos separados por comas. Otra forma es mantener pulsada la tecla «Ctrl» mientras hacemos clic en los diferentes usuarios seleccionados en la lista de contactos. Luego con el botón derecho sobre cualquiera de ellos seleccionamos *Send a message*.

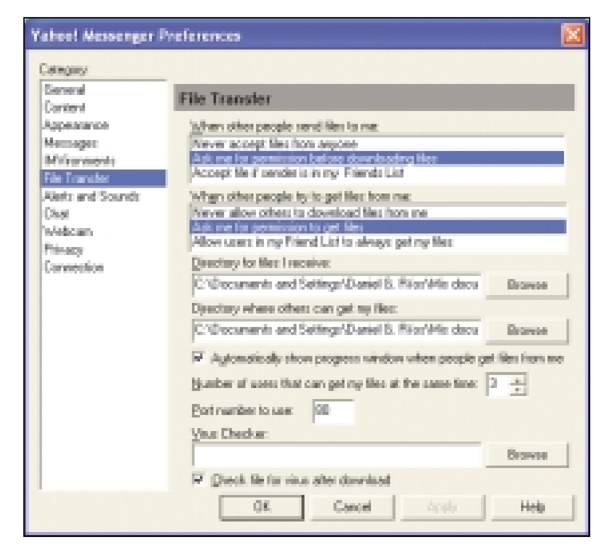
Más mensajes

Pero, ¿qué ocurre si mandamos un mensaje a un contacto que «pasa de nosotros»? Pues que Yahoo! Messenger nos proporciona una interesante función denominada *Buzz* que hará que tanto nuestra ventana como la suya vibren y emitan un sonido zumbante para llamar su atención. Otra opción disponible para captar un momento inolvidable en una conversación es la de imprimir en papel la misma. Esto lo podemos hacer si nos dirigimos a *File/Print*. Por otro lado, si en lugar de iniciar nosotros una conversación, es al contrario, una ventana de texto nos aparecerá automáticamente en nuestro escritorio. Si no queremos responder, tan sólo tenemos que cerrarla. Si no queremos recibir ningún mensaje suyo en el futuro, debemos seleccionar *Ignore User*. Esto hará que no recibamos ningún mensaje de esa persona en el futuro hasta que no la eliminemos de nuestra lista de «ignorados». Si queremos que la ventana de texto de una conversación permanezca por encima de todo el resto de ventanas, tendremos que dirigirnos a *Login/Preferences/General/Keep Yahoo! Messenger on top of all other applications*. En este sentido, Yahoo! Messenger tiene una buena política de seguridad y privacidad. Sin embargo, tenemos que tener en cuenta que una conversación puede ser difundida a otros por nuestro contacto, o incluso una tercera persona puede «interceptar» la conversación, como por ejemplo nuestro administrador de red. Además, como Yahoo! Messenger permite a los usuarios archivar, imprimir y salvar los mensajes, estos historiales son susceptibles de ser espiados por terceras personas.



Compartir archivos

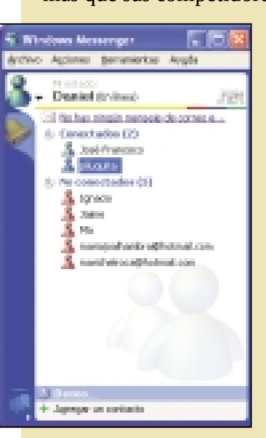
Una de las novedades de las últimas versiones es la opción de compartir archivos con otros amigos. Para configurar esto debemos ir a *Login/Preferences/File Transfer*. Lo primero que haremos será establecer permisos para cuando otras personas nos quieran mandar sus ficheros. Seguidamente elegimos el directorio de intercambio. Después seleccionamos el puerto para el intercambio, que por defecto es el 80. Por último, tenemos la casilla de *Check File for virus after download* que sólo estará hábil si tenemos instalado un antivirus. Por otro lado, para ver los archivos compartidos de nuestro contertulio, debemos hacer clic con el botón derecho sobre su nombre y seleccionar *View Shared Files*. Esto envía una petición a la otra



parte para que nos admita en su lista. Una vez que hemos pasado estos trámites, veremos la lista completa de ficheros y sólo tenemos que seleccionar uno y pinchar en *download*.

Windows Messenger

Este programa de mensajería instantánea de Windows siempre ha tenido el handicap de ser «sólo» el tercero más usado y de que tanto ICQ como la herramienta de Yahoo! tengan más usuarios. Con esta «motivación» ha ido mejorándose versión tras versión, intentado ofrecer más que sus competidores. La realidad es que casi nunca ofrece nada nuevo, limitándose a copiar las nuevas funcionalidades de sus rivales. Y aunque ya está solucionado, este Windows Messenger siempre tenía muchos problemas de conexión y eran habituales las desconexiones Aun así, la última versión, de serie con Windows XP, es muy competitiva. Por lo demás, podremos hacer casi de todo con este *messenger*: voz, vídeo, compartir aplicaciones, etc. Además, se han potenciado mucho los *smileys* y ahora la lista y la calidad es mucho mejor.



No te lo pienses más...
...ya hay una revista a tu medida



Suscríbete a  y/o computer idea y aprovecha estas ofertas

Puedes hacerlo mediante:

 **E-mail:** suscrip@bpe.es

 **Fax:** 913 273 704

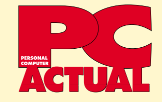
 **Teléfono:** 913 137 900

 **Correo:** COMPUTER IDEA o PC ACTUAL Apdo nº 611 FD. 28080 Madrid

Corta este cupón por la línea de puntos y envíalo por correo.

 *Sí, quiero suscribirme a la/s revista/s beneficiándome del descuento elegido:*

Marca la opción que prefieras

		
Suscripción 1 año	❑ 20% de descuento 11 ejemplares por sólo 43,6€ (7.254 ptas)	❑ 20% de descuento 12 ejemplares por sólo 16,8€ (2.795 ptas)
Suscripción 2 años	❑ 25% de descuento 22 ejemplares por sólo 81,6€ (13.577 ptas)	❑ 30% de descuento 24 ejemplares por sólo 29,5€ (4.908 ptas)

Nombre y apellidos ....

E-mail ....

Dirección de envío. ❑ Particular

❑ Empresa (nombre) ....

Dirección ....

Código postal ....Población ....

Teléfono..........Móvil ....Fecha de nacimiento |_|_| |_|_| |_|_|

Profesión/estudios ....

Información sobre datos personales: ver recuadro al pie de esta página.

Forma de pago:

❑ Adjunto cheque a nombre de **VNU BUSINESS PUBLICATIONS ESPAÑA, S.A.**

❑ Contra reembolso (+300 ptas –1.8 €– por gastos de envío)

❑ Con tarjeta de crédito:

❑ AMEX |_|_|_|_| |_|_|_|_|_|_| |_|_|_|_|_|

❑ VISA |_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Fecha de caducidad: |_|_| |_|_|

Firma:

TRIN04

INFORMACIÓN SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES. De acuerdo con lo dispuesto en la vigente normativa le informamos de que los datos que usted pueda facilitarnos quedarán incluidos en un fichero del que es responsable VNU Business Publications España. C/ San Sotero, 8. 28037 Madrid, donde puede dirigirse para ejercitar sus derechos de acceso, rectificación, oposición o cancelación de la información obrante en el mismo. La finalidad del mencionado fichero es la de poderle remitir información sobre novedades y productos informáticos, así como poder trasladarle, a través nuestro o a través de otras entidades, publicidad y ofertas que pudieran ser de su interés. Le rogamos que en el supuesto de que no deseara recibir tales oferta nos lo comunique por escrito a la dirección arriba indicada.

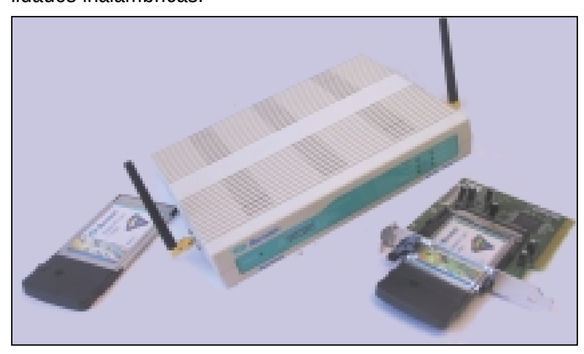


Redes inalámbricas en la empresa

Romper con los cables en la empresa

Raro es el entorno corporativo que no se aprovecha de las ventajas de las comunicaciones en red de equipos informáticos. Buena cuenta dan de ello empresas como Cisco o 3Com, cuyos beneficios multimillonarios recaen sobre las ventas derivadas de este tipo de productos con orientación profesional.

Por pequeña que pueda ser, cualquier oficina que se precie dispone de al menos una red que le permita compartir los recursos de sus sistemas e incluso de Internet. Las empresas, hasta hace bien poco con el obligado cable como protagonista, encuentran ahora una nueva dimensión cargada de posibilidades inalámbricas.



Si bien es cierto que hoy por hoy lo más práctico es hacer uso de una red de cobre, por su alta eficiencia y bajo coste, existen ocasiones en las que la implantación de una red inalámbrica o mixta se revela como más que interesante.

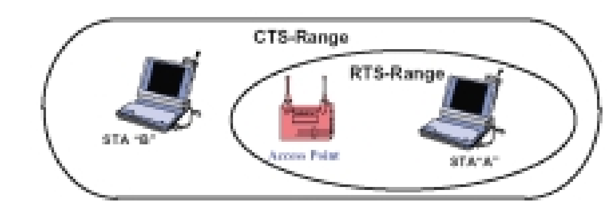
Los entornos ofimáticos suelen estar preparados para afrontar sin problemas la acogida o implantación de la estructura de cables que da soporte a las comunicaciones entre sistemas informáticos. Desde los techos o suelos falsos, a las canaletas que se adhieren a los rodapiés, todos constituyen conductos fácilmente aprovechables para los menesteres de los enlaces informáticos.

No obstante, planteamos una situación más corriente de lo que pueda parecer en un principio. Hay ocasiones en las que prima la necesidad de construir una infraestructura capaz de dar soporte a las necesidades laborales de una oficina en un espacio de tiempo muy limitado. Contactar con técnicos que realicen las modificaciones e instalaciones necesarias, puede provocar problemas difícilmente salvables si no contamos con el tiempo a nuestro favor. Aquí encontramos la primera de las ventajas que nos aportan las nuevas redes inalámbricas, pues en un periodo de pocas horas, dependiendo del número de puestos a instalar, es posible acomodar toda una complicada red de equipos en diferentes plantas, o incluso edificios, sin tener que recurrir a la engorrosa y cara operación del cableado.

Por otro lado, la filosofía móvil que siempre han tenido los ordenadores portátiles ha encontrado un serio lastre en el apartado de las comunicaciones, que requerían hasta ahora un enlace físico con la red de la oficina para intercambiar archivos o para acceder al *router* que daba acceso a Internet. Este aspecto ha constituido el mayor punto de explotación de los nuevos productos inalámbricos, pues tienen una gran aceptación entre los usuarios de informática móvil.

Planteamiento de una red corporativa mixta

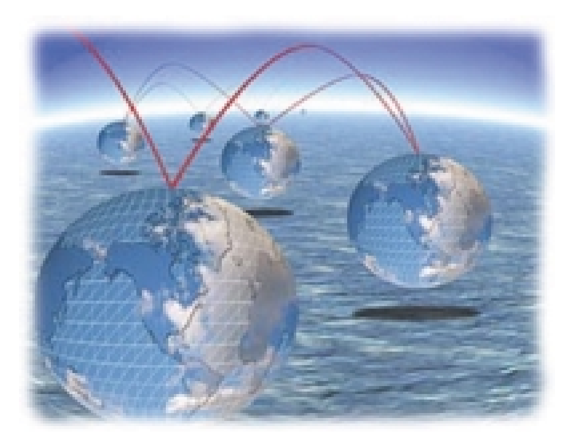
La pregunta obligada a estas alturas es la que surge sobre la manera de resolver el enlace de dispositivos *wireless* con la estructura de comunicaciones de cable. Esto no constituye hoy en día ningún problema, pues entre las soluciones que nos dan los fabricantes se encuentran los denominados puntos de

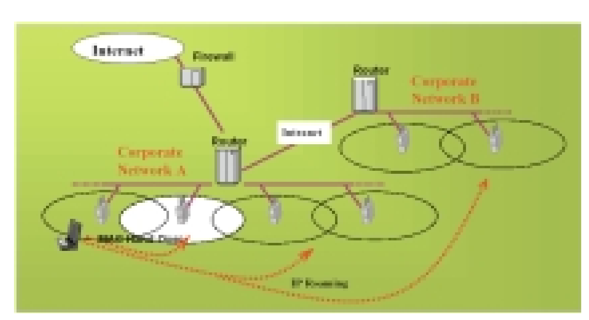


Productos inalámbricos

	3Com	Compaq	D-Link	Enterasys
Modelo del punto de acceso	AirConnect	WL400	DWL-1000AP	RoamAbout
Modelo de la Tarjeta PCCard	Airconnect PC Card	WL100	DWL-650	RoamAbout
Teléfono del fabricante o distribuidor	3Com 91 509 69 00	Compaq 902 10 14 14	D-Link 93 496 57 51	Enterasys 91 405 71 10
Web	www.3com.es	www.compaq.es	www.dlinkiberia.es	www.enterasys.com
Velocidad	11 Mbps	11 Mbps	11 Mbps	11 Mbps

acceso. Estos no son más que unos aparatos que sirven de intermediarios entre ambos tipos de enlaces.
Con una conexión RJ45, que servirá para anclar el dispositivo a la infraestructura de cobre y sus aptitudes inalámbricas, se gestionará fácilmente el proceso de peticiones y comunicaciones con los equipos que se encuentren conectados a la malla física.
La situación de este aparato debe plantearse concienzudamente, pues de esto dependerá un óptimo funcionamiento del sistema de comunicaciones. Hay que tener en cuenta que toda la información que vaya o venga de cualquier punto de red *wireless* pasará a través del aparato. Además, estos puntos de acceso constituyen auténticos repetidores.
Como la cobertura que dan sus características de radiofrecuencia es esferoidal, lo apropiado es situarlo en un punto centrado de la oficina.





Una ubicación elevada, como por ejemplo encima de una estantería o armario, será la más adecuada para dar el máximo alcance. En el caso de que deseemos enlazar varias plantas, lo más interesente será instalar, al menos, uno de estos aparatos por cada piso.
Si además la extensión de la superficie es amplia y alcanza distancias superiores a los veinte metros, necesitaremos la presencia de más puntos de acceso.

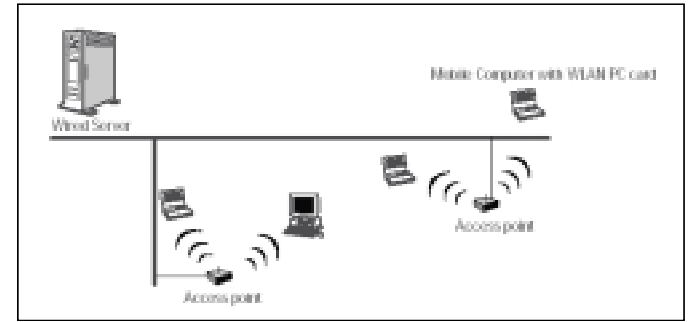
Nuevas posibilidades

Quizás las mayores utilidades que se pueden encontrar en los entornos corporativos son las anteriormente mencionadas posibilidades móviles. En este sentido encontramos un amplio abanico de productos de distintos fabricantes capaces de satisfacer cualquier tipo de exigencia particular.
Aunque los portátiles admiten cualquier dispositivo con interfaz USB, lo más apropiado para estos menesteres es optar por una tarjeta PCMCIA, ya que, al insertarse dentro del PC, evitará posibles engorros a la hora de transportar el ordenador cuando esté encendido, trabajando o descargando archivos de Internet.

Otro de los apartados potencialmente explotables en el mundo de las conexiones 802.11b profesionales es de los nuevos asistentes personales (PDA). Éstos, que tienen la posibilidad de insertar tarjetas PCMCIA, son capaces de comunicar con PC, portátiles, etc., de una manera totalmente móvil y exenta de las ataduras de los cables. Éstos también adquieren por tanto capacidades de acceso a Internet a través del *router* de la oficina, aunque para ello tendremos que tener instalado correctamente el navegador necesario.

Seguridad en el aire

Este aspecto de este tipo de redes ha sido el más polémico desde que empezaron a implantarse de forma masiva. Y es que no sólo estamos hablando de cortar el acceso a nuestros ficheros o recursos compartidos de los equipos que compongan la red. Cualquier equipo con alcance suficiente y una tarjeta de red puede acercarse a alguno de los puntos de acceso y «robar» el ancho de banda que utilizamos para conectar la red a Internet con otros fines muy diferentes. Al tratarse de un medio completamente libre, es necesario implantar algún tipo de seguridad, bien sea autenticación fuerte (y dependiendo del nivel de red al que sea aplicada la autenticación, utilizar cortafuegos o no) o cifrado de las comunicaciones. El ideal



supondría utilizar una combinación de todas estas técnicas. Así, por ejemplo, nuestros puntos de acceso no sólo deberían utilizar WEP (*Wireless Equivalent Privacy*), además éstos no deberían permitir ningún tipo de comunicación con las estaciones que no utilizaran este sistema (evitando así posibles «conductores hackers»). Otra medida de seguridad recomendada sería la implantación de autenticación a nivel de MAC (dirección física del dispositivo de red), es decir, aquellas estaciones con una dirección física desconocida no podrían utilizar el punto de acceso. Como último recurso conviene que los administradores de red se planteen la incorporación de algún tipo de IDS (*Intrusión Detection System*) e incluso situar un cortafuegos en el segmento que comunica la red inalámbrica de la red cableada.

Lucent	Macromate	SMC	Zoom Air
AP-1000	MAP-811	EZ Connect Wireless AP SMC2652W	n.d.
Orinoco Silver Card	MWN-711	SMC2632W	Air Wireless Networking
Lucent 91 714 86 02	Micro BR Comunicaciones 902 15 49 57	SMC Networks 91 320 28 84	UMD 902 128 256
www.orinocowireless.com	www.macromate.com.tw	www.smc.com	www.zoom.com
11 Mbps	11 Mbps	11 Mbps	11 Mbps



Redes inalámbricas en el hogar

El principio del fin de los cables

Los beneficios de comunicar diferentes ordenadores para compartir archivos, programas, conexiones a Internet, etc., son incuestionables. Las comunicaciones entre ordenadores, que hasta hace relativamente poco constituían un apartado de la informática reservada a entornos corporativos, se hace cada día más «hogareña» y comienza a formar parte de innumerables viviendas. Los usuarios encuentran cada vez menos trabas para construir e instalar su propia red de comunicaciones en casa, y está surgiendo una nueva necesidad de comunicación entre los consumidores de productos informáticos.

A la hora de abordar la instalación de una red doméstica, hay que afrontar una serie de problemas de manera ineludible. Quizá el más importante sea el de crear la infraestructura de cables necesaria para que se puedan mantener las comunicaciones entre los diferentes equipos. Los hogares son casi siempre almacenes de muebles, cuadros y elementos ornamentales que dificultan seriamente el trazado y la instalación de la malla de cobre. Si a esto le añadimos el componente estético que marca las reglas del buen gusto, y que incompatibiliza la práctica «chapuza», encontramos que en ocasiones es bastante difícil hallar una buena solución para implementar una red doméstica.

No obstante, los avances tecnológicos no pasan desapercibidos para ningún entorno y la reciente modalidad *wireless LAN* puede suponer un salto a este impedimento.

Detrás de tan exótico nombre se esconde un tipo de redes que no requiere un soporte físico para mantener transferencias de datos entre los sistemas. Utilizando las hondas hertzianas como medio, las tarjetas de red inalámbricas son capaces de establecer comunicaciones sin el engorroso proceso de la instalación de los cables. Si bien es cierto que su precio es considerablemente superior al de dispositivos convencionales, y su rendimiento no alcanza las prestaciones que dan sus primas cableadas, la rentabilidad y la utilidad queda asegurada desde el momento en que permite adaptarse de una manera muy sencilla a cualquier tipo de entorno.





En el mercado existen infinidad de productos y configuraciones con diferentes prestaciones que cumplirán con todo tipo de exigencias particulares. Sin embargo, en todas ellas encontramos una serie de características y denominadores comunes que explicaremos con detenimiento para que os hagáis una idea fiel de lo que supone esta novedosa tecnología.

El estándar 802.11b

Éste es el estándar en el que se definen todas las reglas necesarias para la correcta comunicación de estos dispositivos inalámbricos. En él se establecen las normas que rigen la frecuencia de emisión, de recepción, velocidad de transmisión de datos, encriptaciones y un largo etcétera, imprescindible para un buen entendimiento entre los puntos de red.

Quizá el apartado más importante sea el que dicta la velocidad de transmisión de datos. Actualmente los límites físicos de la comunicación 802.1b determinan como máximos teóricos de picos de comunicación velocidades de «tan sólo» 11 Mbps (millones de bits por segundo). En comparación con los 100 que pueden alcanzar las redes de soporte de cobre, se quedan bastante lejos en cuanto a sus prestaciones, máxime si se tiene en cuenta que estos 11 Mbps son simplemente teóricos, pues según nuestras experiencias quedan reducidos en la práctica a unos 3 Mbps.

No obstante, esto no debe de suponer un desánimo para ningún usuario doméstico, pues cumplen con creces cometidos de comunicación entre juegos y el intercambio de archivos.

Además, si la utilizamos como medio para dar soporte a varios equipos con una sola línea de comunicación con Internet, su «baja» velocidad no supondrá un freno ni para las rapidísimas líneas ADSL de 2 Mbps.
Conviene también tener en cuenta que la velocidad se ve reducida proporcionalmente a medida que nos alejamos entre los distintos puntos de red.

Planteamiento e instalación de una red inalámbrica en casa

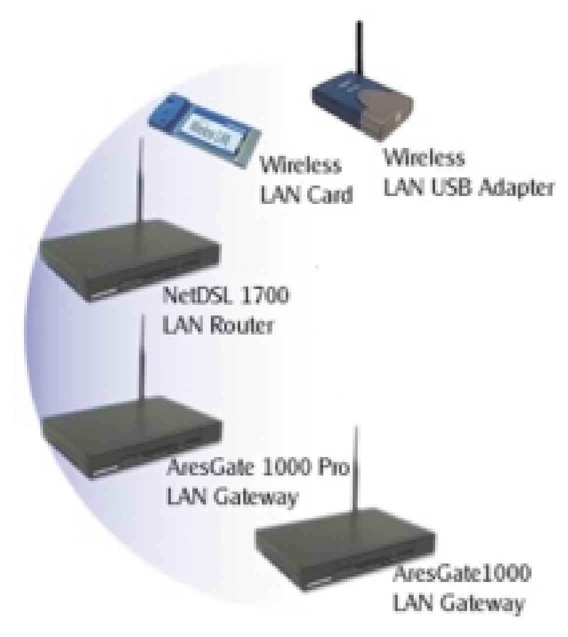
La instalación de cualquier tipo de red inalámbrica no tiene por qué acarrear mayores problemas. Lo primero que tenemos que hacer para instalar una infraestructura de estas características es proceder a la implantación de los componentes hardware. Para ordenadores de sobremesa encontramos en el mercado dos tipos de dispositivos: las tarjetas PCI, que se integran en el interior del ordenador, y los dispositivos externos con conexión USB. Si bien es cierto que no existe una característica importante que las diferencie sustancialmente, las externas tienen mayores posibilidades al poder ser orientadas fácilmente para conseguir una óptima comunicación. Por el contrario, las tarjetas internas quedan descubiertas por su antena en la parte trasera del ordenador, parte que en ocasiones se encuentra inaccesible por estar oculta. Este aspecto puede llegar a dificultar las transmisiones.



En cualquier caso, su instalación puede ser tan simple como la inserción del dispositivo en una ranura libre de la placa madre o la conexión del aparato en uno de los puertos USB.
Posteriormente habrá que proceder a la configuración software con los *drivers* que nos suministra el fabricante. Este proceso no suele dar ningún tipo de percance, y tan sólo deberemos seguir los pasos que se nos van mostrando secuencialmente durante todo el proceso.

Consideraciones

Si nos encontramos en condiciones de poder elegir más o menos libremente la ubicación de los equipos, será recomendable organizarlos de manera que se encuentren todos lo más cercanos posibles. No será necesario preocuparse por otros aparatos como televisores, receptores de radio, etc., pues su frecuencia de trabajo no entorpecerá el desempeño de las actividades de los dispositivos de la red.
La distancia típica de alcance máximo entre dos puntos de red inalámbricos es de unos 100 metros, aunque esto implique la inexistencia de muros o tabiques que deformen la señal a su paso. Si tenemos que unir dos elementos que se encuentran muy distantes, lo mejor será interponer en el medio otro punto de red, pues según las normativas y nuestra experiencia, éste hará de repetidor y enlazará sin problemas ambas comunicaciones.



Existen, dependiendo del fabricante, accesorios como antenas o amplificadores entre otros elementos, que mejoran las comunicaciones en aquellos entornos en los que se requieren instalaciones distantes. Por eso es importante plantear la red antes de proceder a la adquisición de cualquier producto. En el caso de que queramos conformar el sistema de comunicaciones con el vecino del al lado, que comparte nuestra afición por los juegos en red por ejemplo, lo mejor será adquirir uno de estos complementos que aseguren el buen funcionamiento y la transferencia «alegre» de los datos entre las dos viviendas.
Otro punto a tener en cuenta en este tipo de redes es el de la seguridad. Al no contar con un soporte físico y definido que canalice la comunicación, las transmisiones son fácilmente interceptables. Un equipo portátil con funciones *wireless LAN* suficientemente cercano a nuestros sistemas y un programa *Snifer* pueden constituir los elementos más que necesarios para realizar un completo acto de espionaje informático.
Si en casa no trabajamos con documentos críticos, y lo peor que nos puede llegar a pasar es que el vecino nos intercepte el correo, este es un aspecto que podremos pasar por alto. En caso contrario, lo mejor será adquirir un programa encriptador que cifre los documentos a enviar y traduzca los recibidos. Este proceso no ralentiza en exceso las transmisiones, y por lo tanto es muy aconsejable. Su precio no suele ser impedimento para su implantación y la instalación y manejo se hace bastante simple.

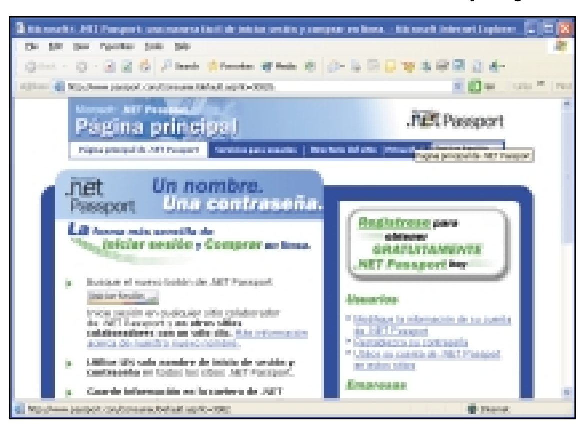




Pasaporte para Internet

Cómo funciona el servicio de autenticación de Microsoft

Passport es el servicio *on-line* de autenticación de usuarios de Microsoft. Permite a un usuario iniciar sesión bajo una única identidad que se corresponderá con su dirección de correo electrónico habitual y una sola contraseña que será reconocida por múltiples sitios web durante la sesión de navegación, teniendo de esta manera un acceso más fácil y seguro a



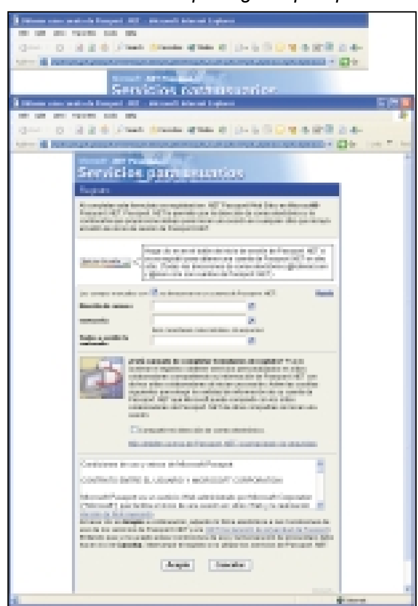
todos los sitios web y servicios que tengan implementado este servicio. En *www.passport.com/directory* podemos encontrar un listado de los sitios web que tienen implementados los servicios de inicio simple de sesión o compra rápida de Passport.

Servicios de Passport

Passsport ofrece dos servicios. El primero de ellos se llama *Single Sign IN* (SSI) y permite al usuario crear una identidad protegida por contraseña en el sistema Passport, acompañado por un perfil como es el nombre, edad, sexo, etc. Los usuarios pueden iniciar sesión bajo su identidad al comienzo de una sesión de navegación web, y después visitar una serie de servicios capaces de reconocer el estatus de su Passport y recibir sus datos de perfil directamente, en vez de preguntar una y otra vez un nombre de usuario y contraseña específicos para cada uno de los sitios web. Estos perfiles de usuario se almacenan en los servidores centrales de Passport en posesión de Microsoft. El segundo servicio que ofrece es *Compra rápida* (Express Purchase), y está dirigido a los sitios web de comercio electrónico. El usuario de Passport puede almacenar los números de sus tarjetas de crédito, direcciones de facturación y de entrega en la cartera de Passport, una extensión del servicio en forma de billetera virtual cuyos datos también se encuentran en los servidores centrales de Passport en la dirección *wallet.passport.com*.

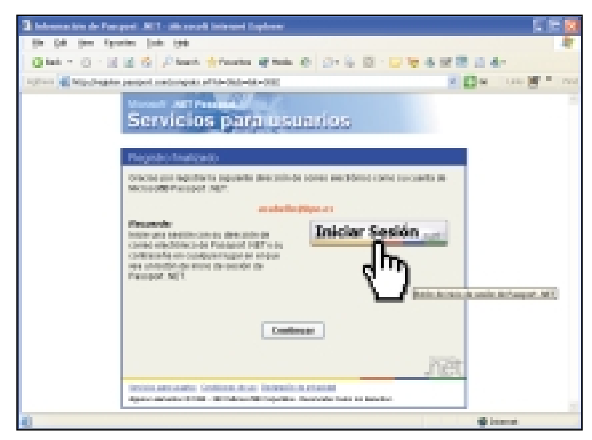
Obtener nuestro Passport

Cualquiera puede obtener una identidad gratuita de Passport visitando la web de registro en español introduciendo la dirección *http://register.passport.com/reg.srf?lc=3082* en nuestro navegador, si bien muchos de los usuarios de este sistema ya lo son actualmente si cuentan con una dirección de correo en el servicio gratuito de Microsoft Hotmail o de MSN, y que obtendrán automáticamente su Passport introduciendo la dirección de correo electrónico y la contraseña del mismo. Para asociar un Passport a nuestra dirección habitual de correo electrónico, rellenaremos el formulario introduciendo y verificando una contraseña que no tiene por qué ser la asociada a nuestra cuenta de correo electrónico. También debemos elegir una pregunta secreta en el cuadro de la lista desplegable y escribir la respuesta en el campo *Respuesta secreta*, datos que serán utilizados en el caso que olvidemos nuestra clave de acceso al servicio Passport.



Compartir nuestros datos

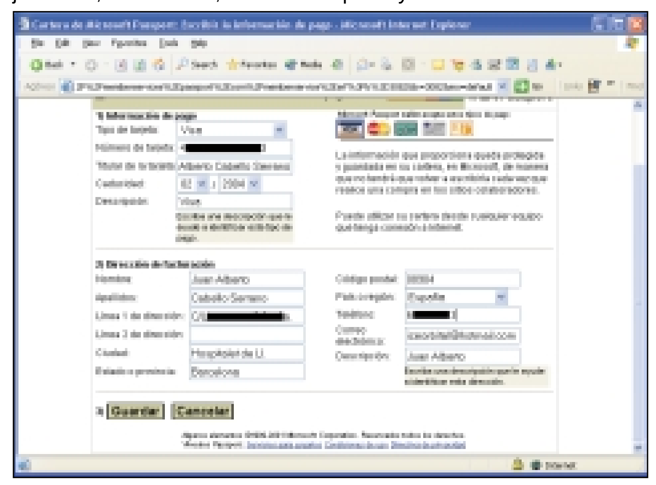
Una parte importante pero opcional de nuestro registro en el servicio Passport es el nivel de confidencialidad que deseamos para nuestros datos de registros. Los únicos datos personales del usuario obligatorios son la *Provincia* y *País* de residencia; si bien todos los datos adicionales que introduzcamos podrán ser utilizados por los sitos web participantes para personalizar sus páginas web con contenidos adaptados a nuestros gustos, aficiones, etc., así como también para acelerar el registro, ya que los campos introducidos en nuestra cuenta de



Passport serán directamente emitidos al formulario de registro del sitio web. Para ello marcaremos una o ambas casillas *Compartir mi dirección de correo electrónico* y *Compartir el resto de mi información de registro*. Tras aceptar los términos de la licencia del servicio, habrá finalizado la configuración de nuestra cuenta de Passport.

Cartera de Passport y servicios para usuarios

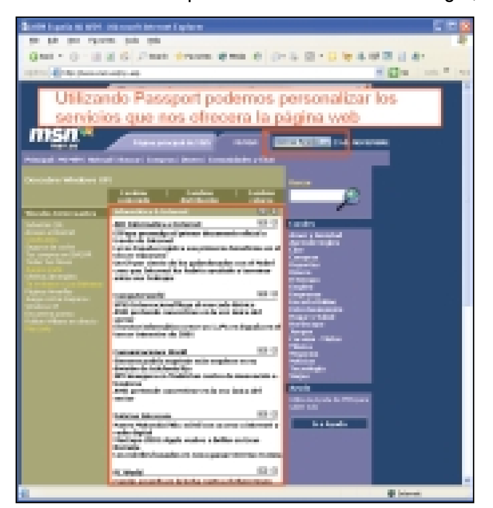
En este momento tenemos la posibilidad de cerrar la ventana del navegador y comenzar a utilizar el servicio de Passport o bien continuar el registro creando nuestra cartera de Passport. En ese caso, en la nueva ventana pulsaremos sobre el enlace *Crear o modificar mi cartera de Passport*, en la que introduciremos los números de nuestra tarjeta de crédito principal o tarjeta de débito que no requieran un número de identificación personal (PIN). La cartera de Passport acepta números de tarjeta VISA, MasterCard, American Express y Diners Club. También introduciremos la dirección de facturación, que será la utilizada para enviar las compras que realicemos. Tras pulsar sobre el botón *Guardar*, verificaremos que todos los datos introducidos sean correctos, así como también podemos pulsar sobre el botón *Nueva* en cada uno de los campos (*Opciones de pago, dirección de facturación y dirección de envío*) para añadir nuevas entradas. Si todo está correcto y no necesitamos añadir más datos, pulsaremos el botón *Listo* para finalizar la configuración. Desde la página principal *Servicios para usuarios* de Passport podremos modificar y completar los datos introducidos durante el registro, con información como la zona horaria, fecha de nacimiento, así como activar la opción de accesibilidad o añadir un número de teléfono móvil



con el que poder ser localizado a través del servicio Windows Messenger y poder iniciar sesión en sitos móviles compatibles con Passport.

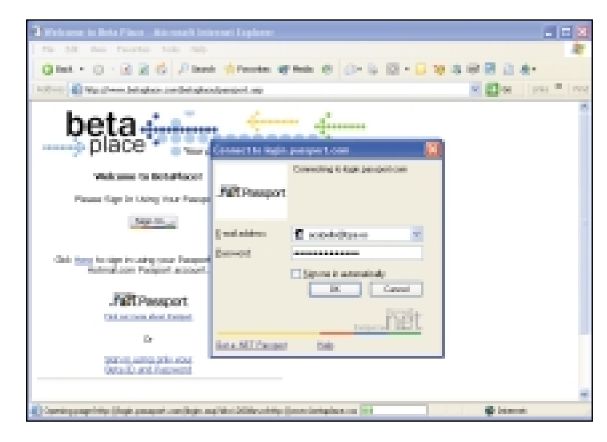
Passport en acción

Los usuarios no tendrán que visitar el sitio web de Passport para iniciar sesión. En su lugar, cada página web compatible con este sistema de autenticación incluirá un botón *Iniciar sesión* (o *sign-in*) en la esquina superior derecha de la página que nos invitará a iniciar sesión usando nuestra cuenta de Passport. Este botón actúa como un enlace dinámico a la página de inicio de sesión de Passport, personalizada con el diseño original del sitio web que estemos visitando que nos pedirá nuestro nombre de usuario y contraseña. Una vez autenticados correctamente, Passport creará una cookie de inicio de sesión en el disco duro del usuario y enviará un mensaje http de redirección para retornar a la página principal del sitio web, en la que ya apareceremos autenticados.



Más comodidad y seguridad

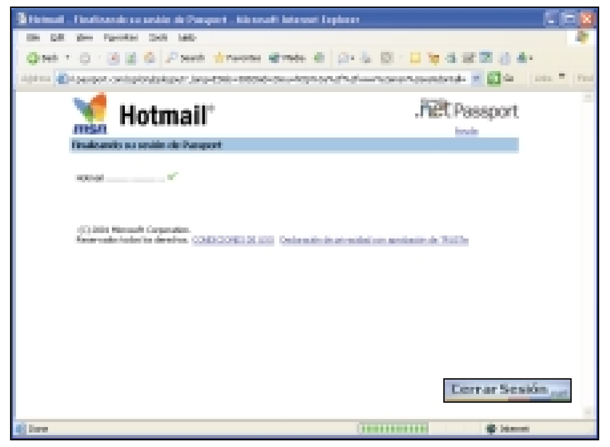
A partir de ese momento, en el próximo sitio web compatible con el servicio Passport que visitemos, el servidor de Passport encontrará la *cookie* de sesión creada anteriormente y no presentará la página de inicio de sesión. En su lugar, y sin que nos demos cuenta de lo que está pasando, el sito web comprobará la existencia de una *cookie* de inicio de sesión en el disco duro del usuario y automáticamente validará esos datos (en un proceso llamado autenticación silenciosa), donde además se crearán las *cookies* específicas y propias del sitio web. De esta manera, se reemplaza el anterior icono *Iniciar sesión* que es sustituido por el de *Finalizar sesión*. A partir de ese momento tendremos iniciada sesión en dos sitios, cada uno manteniendo sus propias *cookies* de datos. Sin embargo, un sitio web puede sortear este mecanismo, insistiendo en que el usuario realice un *hard login* (inicio de sesión duro), que básicamente consistirá en volver a introducir su contraseña cada vez. Estas



son las reglas de Passport. Una vez que el usuario ha pulsado el botón *Iniciar sesión* en un sitio particular, el resto de sitios asumirá que el acceso se realiza desde el mismo perfil de Passport, de forma que no sea necesario volver a autenticarse.

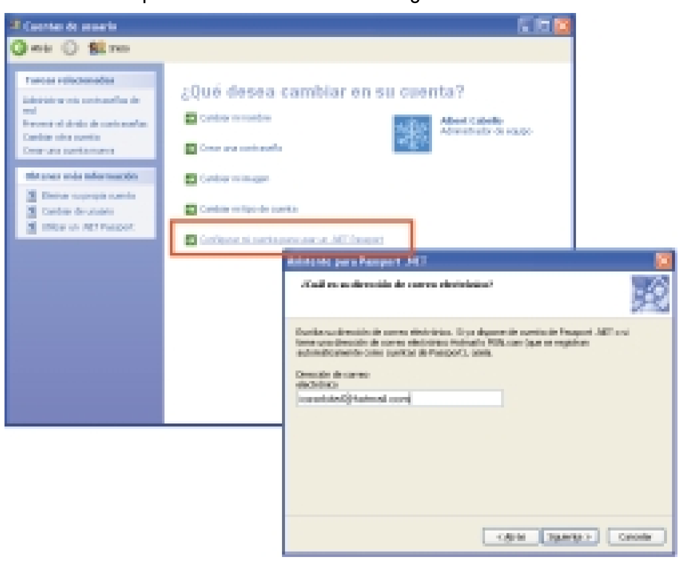
Finalizar sesión

Como ya hemos dicho, cuando un usuario tenga iniciada sesión, el botón que se mostrará en los sitios web será el de *Cerrar Sesión*. Este botón redireccionará la petición a la página de cierre de sesión de Passport. En ese momento, las *cookies* de sesión de Passport, que contendrán una lista de nombres de los sitios web en los que el usuario tiene iniciada sesión, serán procesadas y Passport llamará automáticamente a cada una de las direcciones URL de cierre de sesión para cada sitio web. Estos sitios deberán eliminar su propia *cookie* de sesión y aquellas que contengan datos derivados del uso de Passport. Tras finalizar este proceso con cada uno de los sitios web, éstos devolverán una marca gráfica en forma de «tick» indicando el cierre con éxito de la sesión.



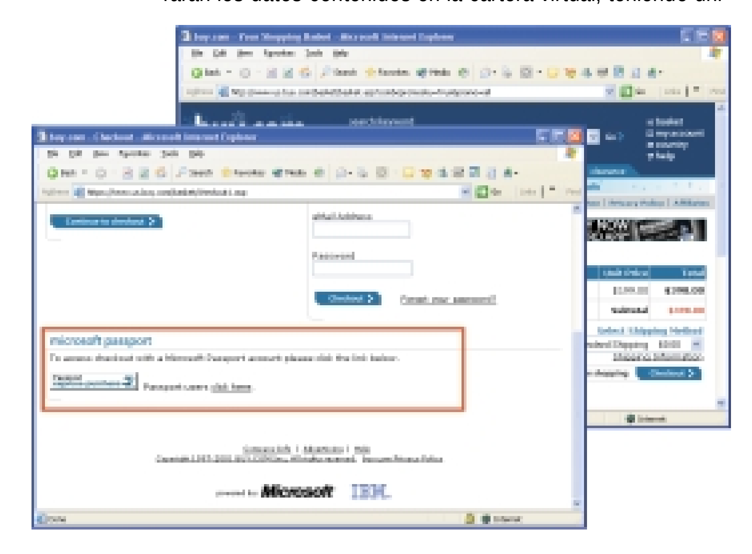
Con Windows XP

Si utilizamos Windows XP, Windows Messenger será el programa que nos invitará a entrar en el mundo .NET y que utilizaremos para autenticarnos en multitud de sitios web así como también para hablar con nuestros amigos. Windows XP permite asociar cada cuenta de usuario local con una cuenta de Passport, lo que nos servirá para autenticarnos en Internet y utilizar servicios como Messenger. De esta manera, al iniciar sesión en nuestro equipo, automáticamente lo haremos también en sitios como Hotmail o MSN y no tendremos que introducir nombres de usuario o contraseñas en estos sitios web para que nos reconozcan como usuarios y nos presenten contenidos personalizados según nuestro perfil. Esta asociación la realizaremos a través del *Panel de control*, pulsando sobre *Cuentas de usuario*, donde tras pulsar sobre un identificador de cuenta de usuario, en el panel de tareas situado en la parte superior izquierda, podremos establecer esta asociación



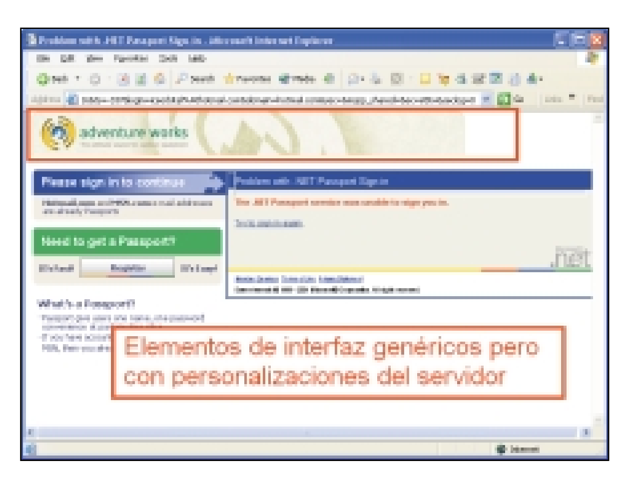
Compra rápida de Passport

Los sitios web que cuentan con esta tecnología muestran un enlace *Compra rápida* (*Express Purchase*) en las páginas de verificación de compras donde automáticamente se recuperarán los datos contenidos en la cartera virtual, teniendo únicamente el usuario que escoger el número de la tarjeta de crédito donde cargar el pago y verificar la dirección de entrega y facturación para finalizar la transacción. No es necesario que vuelvan a escribir números de tarjetas de crédito o preocuparse, ya que los datos viajan por una vía segura entre ambos servidores.



Passport en el servidor

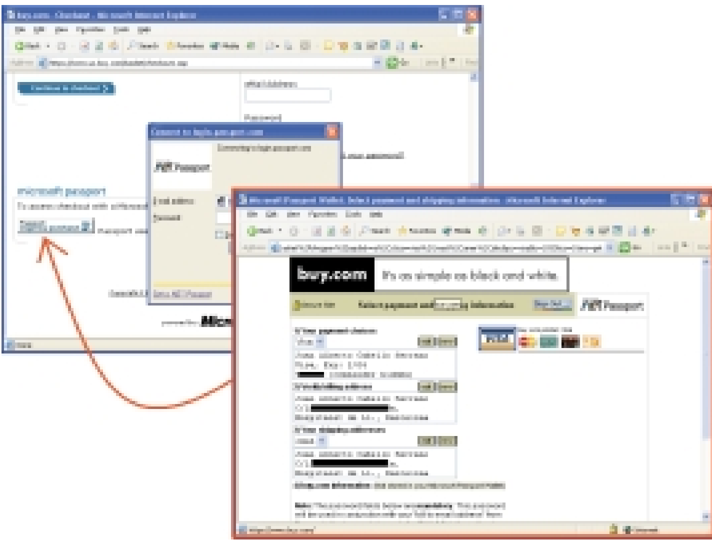
El sistema de páginas de Passport contiene unos elementos de interfaz genéricos, como son el formulario para la introducción del nombre de usuario y contraseña, y siempre serán ejecutados desde los servidores centrales de Passport. Sin embargo, pueden incluir algunos elementos personalizados que ayuden a integrarse visualmente dentro del sitio web que hace uso de estos servicios. Esto es posible gracias a unas plantillas en las que el servidor ejecuta una serie de Javascripts. Al autenticarse un usuario, los sitios web recibirán una identificación codificada en una clave de 64 bits, directamente del servidor de Passport, conjuntamente con una cantidad limitada de datos personales del mismo (los que son obligatorios durante el registro de la cuenta) y en los que nunca se incluirá la contraseña de la misma. En ocasiones los datos utilizados (país, estado, región, código postal...) únicamente lo son para fines esta-



dísticos, ya que el resto (como apodo, nombre real, fecha de nacimiento…) son opcionales y los usuarios pueden decidir mantenerlos en secreto. Además, los usuarios que no tengan una cuenta de Passport serán redireccionados por un sistema integrado dentro del sitio a la página de registro de Passport, en vez de la página de inicio de sesión. No obstante, cuando sea el sitio web el que envíe un usuario a registrarse, podrá especificar algunos campos en el perfil que normalmente son opcionales como obligatorios.

Compra rápida en el servidor

Al contrario que el inicio simple de sesión (SSI), la *Compra rápida* no requiere un software especial en el sito web participante, ni siquiera la necesidad de usar el SSI de Passport, Esto es debido a que la *Compra rápida* realizará su propio inicio de sesión de Passport para poder localizar la «billetera» del usuario, ya que toda la información de la billetera se guarda por separado del perfil de Passport para evitar posibles problemas de seguridad. Passport mostrará una página personalizada con el estilo del sitio web, que permitirá al usuario escoger la tarjeta de crédito y la dirección de facturación y envío a utilizar, información que se enviará de nuevo a la URL del sitio web a través del protocolo HTTPS y utilizando seguridad SSL. *Express Purchase* únicamente realizará una verificación preliminar de los números de las tarjetas de crédito, de forma que la autorización y el proceso de la transacción siguen siendo responsabilidad de los sitios web.



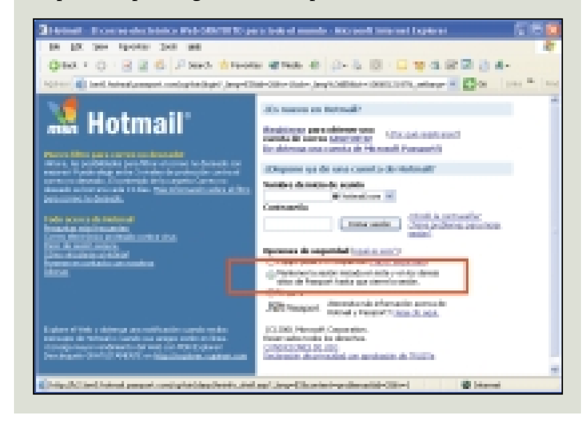
Kids Passport

Kids Passport (*http://kids.passport.com*) es una versión especial de Passport dirigida a los niños, cuya principal novedad radica en que es capaz de proteger la privacidad en línea de los usuarios menores de edad. Kids Passport no funcionará como filtro web para que los niños no accedan a sitios determinados. En su lugar, los padres o tutores controlarán el tipo de información en el perfil de usuario del niño, que será compartida con los sitios participantes y cuando el niño intente iniciar sesión en un sitio compatible con el servicio, serán los padres los que proporcionen el consentimiento a través de éste.



El caso de Hotmail

Algunos servicios que utilizan Passport, como el de correo electrónico Hotmail, permiten que sea el usuario quien decida si la *cookie* de sesión generada podrá ser procesada para el inicio de sesión automático en otros sitios web (en caso de que sea el único usuario del equipo), o si no nos preocupa que otras personas que utilicen el equipo puedan acceder a nuestra información privada. Para ello, encontraremos la opción *Mantener la sesión iniciada en éste y en los demás sitios de Passport hasta que cierre la sesión* en la página *Iniciar sesión*, lo que nos permitirá entrar y salir libremente de estos servicios, iniciando nuestra sesión automáticamente. Sin embargo, para nuestra seguridad es posible que se nos pida la contraseña si volvemos a esta página después de un periodo prolongado de tiempo.

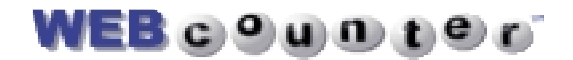




Contadores de visitas

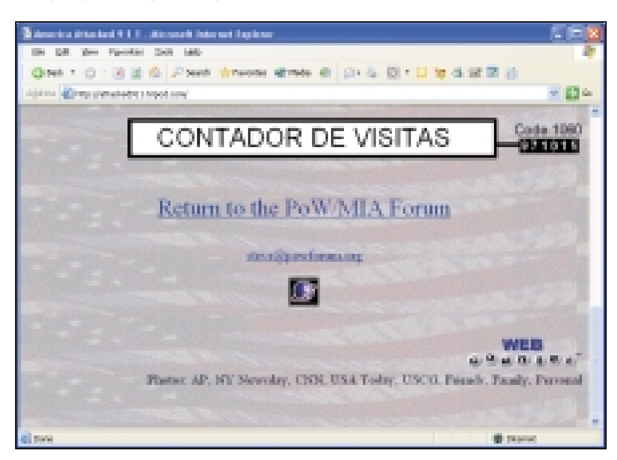
Cómo poner un contador de visitas en una página web

Un contador de visitas sirve para que el usuario de la página web, así como el administrador de la misma, sepan cuántas visitas se han efectuado al web. Visualmente, se trata de una imagen dinámica, que se modifica (en progresión numérica) cada vez que un visitante abre la página en la que reside el contador.



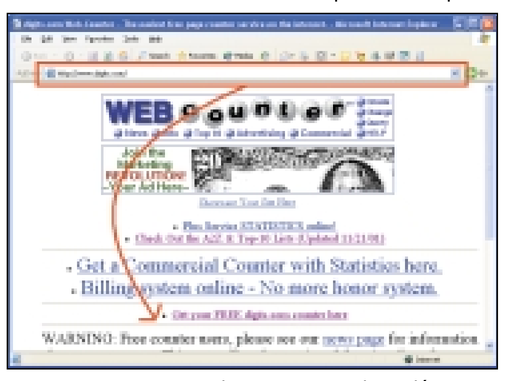
Funcionamiento

Un contador de visitas no se crea con una etiqueta del lenguaje HTML, sino que se genera a partir de un programa CGI especial instalado en el servidor. Puede tratarse del servidor donde esté alojada nuestra página, si es que tiene instalado un programa de este tipo o, en caso contrario, se puede recurrir a otros servidores distintos que den este servicio, como veremos más adelante. En principio, un usuario también podría instalar él mismo un programa CGI en el servidor para hacer uso de él, pero es muy poco habitual que los administradores de los servidores permitan a sus usuarios instalar programas ejecutables debido a los riesgos para la seguridad del servidor que ello supone (como la introducción de virus, por ejemplo). Para instalar un contador de accesos en nuestra página, deberemos colocar una etiqueta que llame a un programa CGI residente en un servidor que nos proporcione este servicio. Estas etiquetas no son un estándar del lenguaje HTML; las ha de suministrar el servidor que ofrezca el servicio porque depende del programa que tenga instalado.



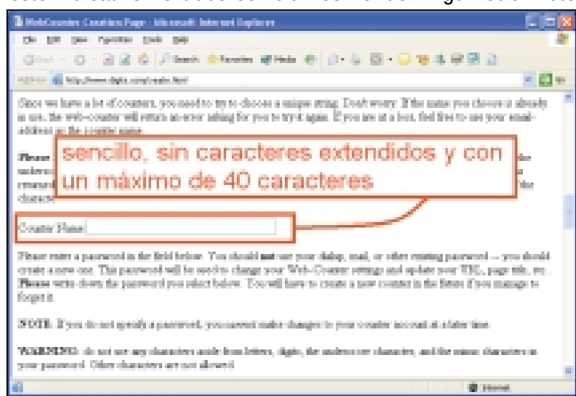
Contratar el contador

Para contratar nuestro contador, lo primero que haremos es introducir en nuestro navegador la dirección *www.digits.com/create.html*, que será el proveedor gratuito que utilizaremos para crear el citado contador. Esta página contiene las instrucciones que nos guiarán paso a paso, así como también nos emplaza a que si utilizamos su servicio gratuito de contadores, insertemos en nuestro web un enlace a dicha página para poder seguir costeando el servicio y mantenerlo de forma gratuita. La lista de los *banners* existentes para publicitar el servicio, así como las instrucciones para su inserción se encuentran en *www.digits.com/-thumbnail/*. Una vez leídos todos los términos, pasaremos a la creación del contador.



Rellenar la petición

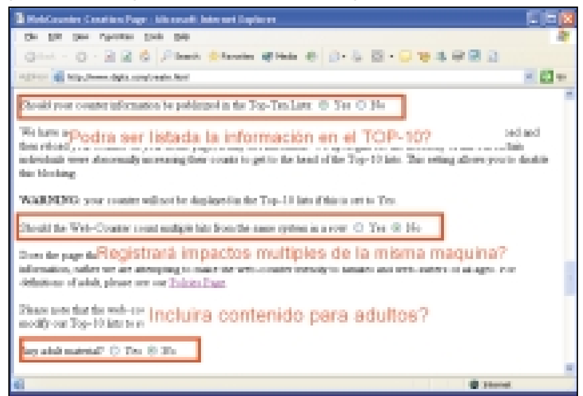
En primer lugar, en el campo *Counter Name* introduciremos el nombre de nuestro contador. Este nombre ha de ser corto y fácil de recordar y, si no es así, automáticamente será modificado por el servidor eliminando los caracteres extendidos con un guión bajo «_» y acortando su longitud hasta un máximo de 40 caracteres. Es muy importante destacar que los nombres son sensibles a las mayúsculas, de forma que «TrucosPCA» no será el mismo contador que «trucospca». Huelga decir que este indicativo no debe coincidir con el de ningún otro. Acto



seguido, introduciremos y verificaremos una contraseña de acceso, que nos permitirá administrar nuestro contador. En el campo *Starting Count* escribiremos el número a partir del que comenzarán a contarse las visitas (normalmente 0, que es la opción predeterminada); por último, introduciremos nuestra dirección de correo electrónico, que es donde se nos enviará toda la documentación necesaria y pulsaremos sobre el botón *Aceptar*.

Ultimando la información del sitio web

Las últimas opciones que debemos rellenar para crear nuestro contador se refieren al sitio web donde lo situaremos. En primer lugar, determinaremos bajo el campo *Should your counter information be publicized in the Top-Ten Lists* si nuestra página web podrá o no ser listada entre las más visitadas, el comportamiento que tendrá frente a múltiples accesos del mismo



sistema en un corto espacio de tiempo (si contará como un único acceso o como varios de ellos), así como si nuestra página web incluirá material para adultos. Por último, introduciremos la dirección URL de la página cuyos accesos queremos contar, normalmente la página principal de nuestro sitio web, así como el título de ésta para que pueda ser listado en la lista de Top-10. Tras pulsar el botón *Create Counter* (Crear contador) en el navegador, aparecerá una página cuyo contenido deberemos guardar en nuestro disco duro, ya que en él se incluyen las instrucciones para la inserción del contador en nuestra página web.

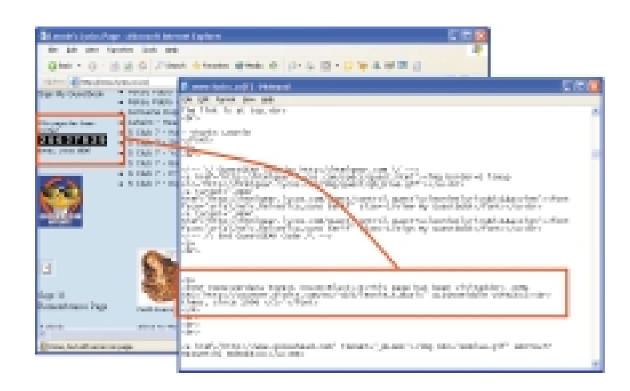
Instrucciones básicas para insertar el contador en nuestra página web

La inserción del contador de visitas la realizaremos desde nuestro editor de páginas web, modificando el código HTML del documento que forma la página principal. La llamada al contador debe incrustarse como una etiqueta más de HTML en el mismo lugar en el que se desea que aparezca la imagen del contador, y ha de encontrarse entre los tags *body* y */body*. Técnicamente, el contador de visitas funciona como una llamada desde la página web a un recurso residente en un servidor; en este caso, *digits.com*.

La etiqueta para un contador creado con el servicio *webcounter.com* tiene la siguiente sintaxis:

<IMG SRC="http://counter.digits.com/wc/-d/4/[nombre_de_contador]">

Como podemos observar, se trata de una etiqueta de imagen. Sin embargo, esta etiqueta no pide al servidor que nos envíe una imagen, sino que llama a un programa instalado en un servidor cuya dirección es http://counter.digits.com y que está instalado en el directorio *wc*. Este programa gestiona conta-



dores de miles de usuarios, pero la llamada de esta etiqueta activa uno en concreto: el que tiene como nombre la palabra *[nombre_de_contador]*. El programa incrementa en una unidad la cuenta y devuelve una imagen con los dígitos correspondientes al número de veces que ha sido activado, utilizando el modelo predeterminado.

Configuración avanzada para la inserción de contadores

Hay muchas opciones que controlan el look resultante de nuestro contador. Cada una de estas opciones adicionales se insertan dentro de *IMG SRC* separándolas del nombre del contador y del resto de opciones con el carácter barra «/». Algunas opciones van acompañan de valores que también se separan con el carácter «/» . Por ejemplo, la opción «–d» requiere un número, de forma que el código HTML quedará transformado de:

<IMG SRC="http://counter.digits.com/wc/[nombre_de_contador]">

a:

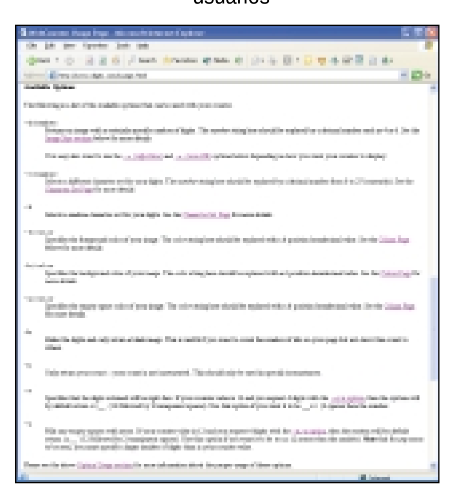
<IMG SRC="http://counter.digits.com/wc/-d/4/[nombre_de_contador]">

Las opciones disponibles para la configuración de nuestro contador son:

-d/[número]: Devuelve una imagen con un número específico de dígitos. La cadena [número] debe ser reemplaza por un número decimal, como 4, 6…

-R: Selecciona una fuente aleatoria para mostrar el resultado del contador.

-h: Esconde lo dígitos y únicamente mostrará una imagen negra. Este ajuste es útil si queremos contar el número de impactos en nuestra página pero sin mostrarlo al resto de usuarios



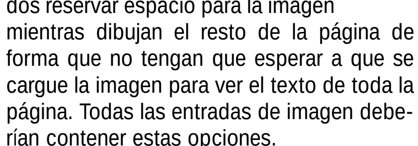
-n: Únicamente retornará el valor de nuestro contador, pero sin ser incrementado.

-r: Especifica la alineación a la derecha de los dígitos retornados en la presentación. Si nuestro contador de visitas es 12 y lo tenemos configurado con 4 dígitos con la opción «–d/4», el sistema retornaría por defecto 12 seguido de dos espacios transparentes. Usando esta opción los espacios en blanco aparecerán antes del número, alineando éste a la derecha

-z: Rellena los espacios vacíos con ceros, de forma que si nuestro contador da un número de 12

y lo tenemos configurado con la opción «–d/4», el sistema que devolvería por defecto la cadena 12 seguida de dos espacios transparentes, devolverá la cadena 0012.

Tamaño del contador



Especificando el número de dígitos con la opción «–d/[número]», sabremos el tamaño de la imagen que retornará nuestro contador. Con esta información, podemos especificar la anchura y altura de la información contenida en la entrada *IMG* que llama al contador. Estos valores permitirán a usuarios más avanzados reservar espacio para la imagen mientras dibujan el resto de la página de forma que no tengan que esperar a que se cargue la imagen para ver el texto de toda la página. Todas las entradas de imagen deberían contener estas opciones.

La altura de la imagen retornada es siempre 20 (*pixels*). La anchura se calcula multiplicando 15 veces el número de dígitos especificados. De forma que si utilizamos la opción «-d/4», la anchura deberá establecerse en 4*15 =60 (*pixels*):

<IMG SRC="http://counter.digits.com/wc/-d/4/[nombre_de_contador]" WIDTH=60 HEIGHT=20>

Un contador de 10 dígitos tendrá una anchura de 10*15=150, la altura será siempre 20:

<IMG SRC="http://counter.digits.com/wc/-d/4/[nombre_de_contador]" WIDTH=150 HEIGHT=20>

NOTA: Si queremos que nuestro contador tenga un tamaño diferente al predeterminado, podremos definir la altura y anchura que deseemos dentro del tag *IMG* y el navegador escalará la imagen de forma automática. No obstante, la imagen se mostrará mejor si los valores de anchura y altura se escalan proporcionalmente. Por ejemplo, en vez de una imagen de 4 dígitos con una anchura de 60 y una altura de 20, podemos establecer su anchura a 129 y altura a 40, doblando el tamaño de nuestro contador.

Modificando la fuente del contador

Existe un buen número de caracteres alternativos para mostrar nuestro contador y que pueden seleccionarse añadiendo el parámetro *–c/[número]*, donde la cadena [número] ha de sustituirse con el valor decimal de uno de los 27 juegos de caracteres que queramos utilizar. Los caracteres disponibles en el servicio Webcounter son varios.

Por ejemplo, para utilizar el primer juego de caracteres alternativos (el predeterminado es «–c/0») utilizaremos el parámetro «–c/1»:

<IMG SRC="http://counter.digits.com/wc/-c/1/[identificador_de_contador">

Modificar el color del contador

También podemos modificar el parámetro que define los colores utilizados por nuestro contador, haciendo uso de los modificadores «–b»(ackground) «–f»(oreground) y «–e»(mpty). Estos modificadores establecen el color de fondo, el de primer plano y el del área vacía. El color de primer plano es el utilizado para los dígitos y se corresponde con el predeterminado blanco (FFFFFF). Los dígitos se muestran en el color de fondo predeterminado negro (000000). El color del área vacía se utiliza para los espacios en blanco que no contienen dígito alguno. Por ejemplo, para utilizar en nuestro contador el color púrpura utilizaríamos.

<IMG SRC="http://counter.digits.com/wc/-c/7/-d/6/-f/A078FF/[identificador_de_contador]" ALIGN=middle WIDTH=90 HEIGH=20>

En este ejemplo, el parámetro «–f» está seguido por la cadena hexadecimal A078FF, que determina el color púrpura. En las dos primeras posiciones, el número hexadecimal define el valor del color rojo (A0), las dos siguientes el verde (78) y las dos últimas el azul (FF). Cada valor de color va desde 00 (oscuro) a FF (brillante), de forma que FF0000 sería el rojo más intenso y 90FF20 sería una combinación de rojo medio, verde brillante y azul oscuro.

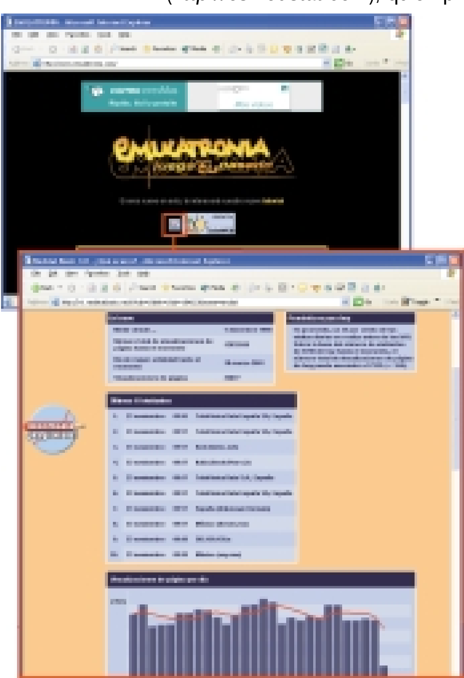
El color predeterminado del área vacía es el verde claro (BEBEBE). Especificando el mismo valor para el color de fondo y el área vacía, el color de fondo se mostrará transparente consiguiendo el efecto de que los dígitos estén flotando en la página. El siguiente ejemplo establece el color de primer plano a verde (00B000) y ambos valores color de fondo y área vacía a blanco (F4F4FF) que es el fondo que solemos utilizar en páginas web.

<IMG SRC="http://counter.digits.com/wc/-rz/-d/5/-c/1/-f/00B000/-b/F4F4FF/-e/F4F4FF/[nombre_de_contador]" ALIGN=absmiddle WIDTH=75 HEIGH=20 BORDER=0 >

Conviene tener en cuenta un detalle importante: el color de primer plano se mezcla con el color de fondo, de manera que deberemos asegurarnos de que el color de fondo de nuestro contador coincida lo más posible con el color de fondo de nuestra página o la imagen.

Estadísticas de las visitas

Además de saber el número de visitas recibidas en una página, es posible conocer las estadísticas detalladas de dichas visitas: por día, por semana, por día de la semana, por hora, por dominio/país, etc., incluso podemos conocer los URL (o direcciones) de las páginas desde donde accedieron las últimas visitas. Todo esto se consigue dándose de alta en NedStat (*http://es.nedstat.com*), quien proporciona este servicio gratuitamente para los usuarios particulares y organizaciones sin fines de lucro. También tiene otro servicio no gratuito para las empresas o sitios de la Web con carácter comercial, que ofrece muchas otras opciones adicionales para poder controlar los accesos a una página. Para darse de alta es necesario rellenar un formulario con los datos personales y de la página web, y acto seguido recibiremos en nuestro buzón de correo electrónico un *e-mail* con el código HTML que hay que insertar en la página. A diferencia del contador, se tratará de una etiqueta que provocará la aparición de un pequeño icono, que una vez pulsado dará acceso a las estadísticas de visitas de la página.

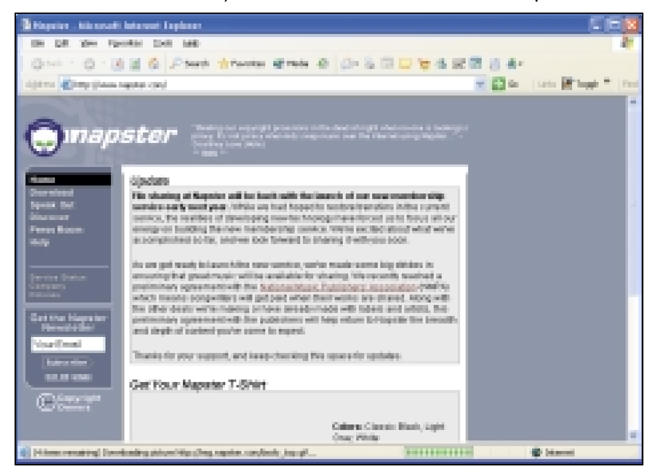




Alternativas a Napster

Busca e intercambia música en Internet

Napster fue un programa que apostó fuerte por un nuevo tipo de filosofía en el intercambio de los ficheros, dejando de lado los servidores tradicionales y haciendo que fueran los propios ordenadores de los internautas los que ejercieran de servidores. De esta forma se aseguraba que todos los archivos encontrados podrían ser descargados directamente sin necesidad de intermediarios. Pero la RIAA (*Recording Industry Association of America*) anunció una demanda contra Napster



por fomentar la piratería en Internet, demanda que al final acabó con el cierre de Napster, hasta mediados del año entrante, en que volverá como un servicio de pago. Desde entonces, muchos de los usuarios de esta herramienta no han encontrado todavía un sustituto a la altura. Sin embargo, Napster no es el único modo de buscar e intercambiar ficheros con otros usuarios a través de Internet. El mayor inconveniente que tenían hasta ahora era la escasez de usuarios: Napster tenía tanto éxito que cada usuario nuevo no se planteaba probar otras alternativas, porque sabía que allí iba a encontrar seguro lo que buscaba. Muchos de los actuales clientes y servidores alternativos a Napster presentan varias ventajas frente al primero: la primera es el cifrado de la información que se envía, en un impulso de mantener el total anonimato; y, por otro lado, la descentralización del servicio, como GNUtella, en que ya no hay un servidor central como en Napster, sino que todo fluye a través de los ordenadores de los usuarios finales. Así no hay ninguna compañía a la que perseguir o demandar. Para atacarlos habría que demandar a miles de desarrolladores o a los usuarios. Por ello hemos preparado una guía explicativa de las mejores alternativas a Napster.

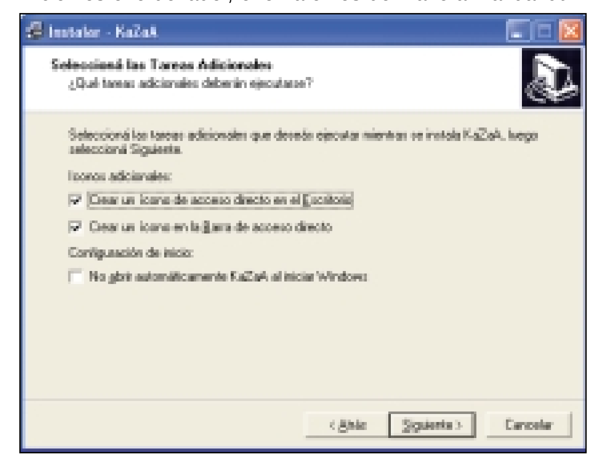


KaZaA

KaZaA es una de las aplicaciones más completas de las existentes actualmente para compartir de una manera rápida y sencilla todo tipo de archivos, y muy similar en su funcionamiento a Grokster (*www.grokster.com*) y Morpheus (*www.musiccity.com*).

Descarga e instalación

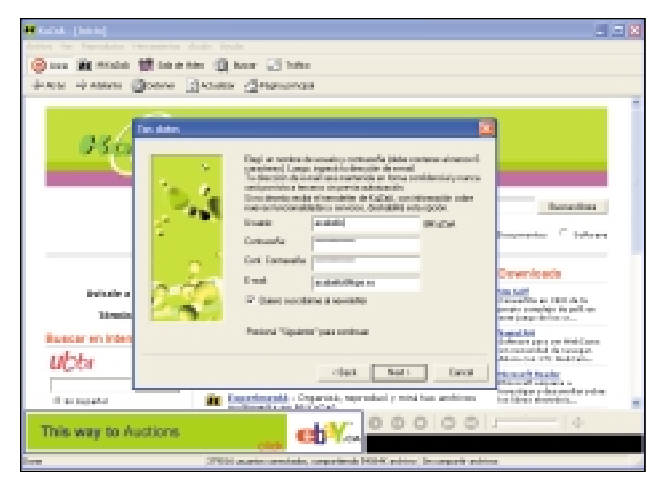
Para el correcto funcionamiento de KaZaA en equipos necesitamos contar al menos con la versión 4.0 de Internet Explorer y Windows Media Player 6.0, ya que estas aplicaciones son utilizadas por algunas funciones del programa. Existe una versión alpha para sistemas Linux así como un *plug-in* para Winamp que permite descargar archivos multimedia para su reproducción en tiempo real. Desde la página web principal de KaZaA (*www.kazaa.com*), encontramos un enlace a la página de descarga, desde la que nos bajaremos la última versión disponible. El archivo descargado es un programa instalador al estilo de los utilizados en las distribuciones de Internet Explorer, donde tendremos que escoger el idioma de entre los cuatro disponibles, incluido el español. Una vez descargado el archivo en nuestro ordenador, se ejecutará automáticamente la instalación del mismo. Tras aceptar el contrato de licencia y especificar un directorio donde se almacena la aplicación, definiremos el número de componentes que se instalarán y la configuración de inicio del programa; donde podemos definir si se lanzará el programa de forma automática cada vez que iniciemos el ordenador, o lo haremos de manera manual utili-



zando los iconos que crearemos en los menús de *Inicio*, *Escritorio* y menú de *Inicio rápido*. Tras estos pasos, dará comienzo la copia de archivos. Una vez finalizado el proceso comenzaremos la configuración del mismo.

Primera conexión y registro

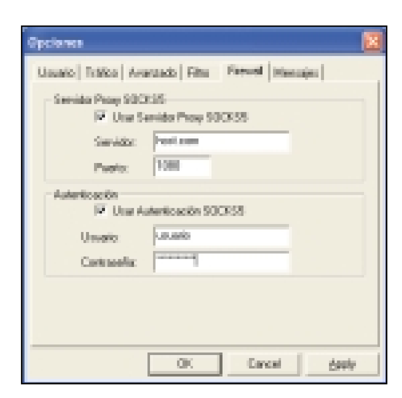
Al iniciar el programa cliente, automáticamente seremos conectados al servidor principal de KaZaA, quien validará nuestra identidad para poder comenzar a compartir archivos. Una de las ventajas que ofrece este mecanismo es que



automáticamente se comprobará la existencia de una nueva versión del programa, pidiendo en ese caso al usuario consentimiento para descargar e instalar la actualización, y asegurarnos de esta forma que tenemos nuestro programa al día y libre de defectos. Como es la primera vez que nos conectamos al servicio, será obligatorio que nos registremos como usuarios, si bien el registro es gratuito y de por vida. Para ello aparecerá un asistente la primera vez que iniciemos el programa. El problema de este asistente es que no contempla a los usuarios previamente registrados, por lo que, si somos uno de ellos, tendremos que cerrarlo pulsando sobre el botón *Cancelar* y, dentro del menú *Herramientas/Opciones de la aplicación*, introducir nuestros datos de usuario y contraseña bajo la pestaña *Usuario*. En el caso de que seamos nuevos usuarios de la aplicación, los únicos datos necesarios para formular el registro será un indentificativo único de usuario, que nos validará frente al servidor y el resto de usuarios, una contraseña de al menos 6 caracteres y la confirmación de la contraseña que verificará la identidad, además de una dirección de correo donde podremos recibir las listas de correos sobre nuevas funcionalidades del programa y otros servicios.

Firewall

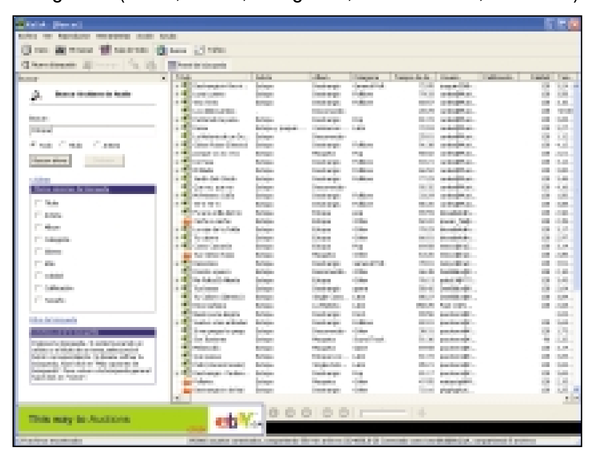
Si nos conectamos a través de un cortafuegos a Internet, podremos seguir utilizando normalmente KaZaA, siempre y cuando configuremos bajo la pestaña *Cortafuegos* del menú *Herramientas/Opciones* los datos necesarios: nombre del servidor, puerto de conexión y si es necesario un nombre



de usuario y *passport* compatible con el servicio de autenticación SOCKS 5.

Motor de búsqueda

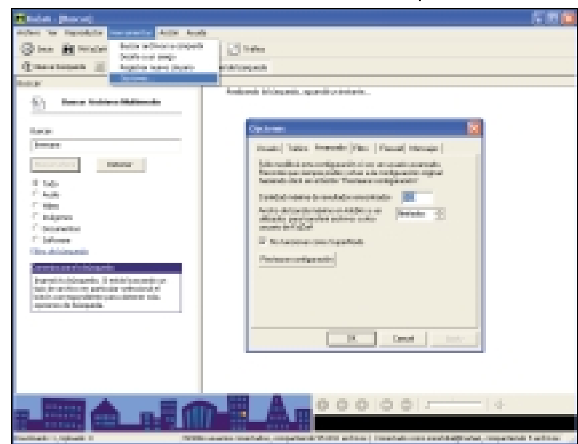
El motor de búsqueda de KaZaA está optimizado para la búsqueda de archivos multimedia (audio, video, imágenes), en los que es capaz de mostrar información extendida como los *tags* ID3 en ficheros MP3. No obstante, en el caso de los MP3, su búsqueda y descarga está limitada por motivos legales a archivos de un máximo de 128 kbps (calidad inferior a CD). No obstante, KaZaA permite compartir todo tipo de documentos y archivos. Para ello la herramienta de búsqueda incluye varias categorías (audio, vídeo, imágenes, documentos, software)



con las que delimitar nuestras búsquedas. Asimismo, podremos ver el tiempo estimado para la descarga de los archivos basado en nuestra conexión y en la del ordenador remoto. Si no encontramos el archivo que buscábamos, podemos intentarlo nuevamente introduciendo una cantidad menor de palabras o seleccionando alguna de las opciones en el apartado *Más Opciones de búsqueda*.

Resultados en la búsqueda

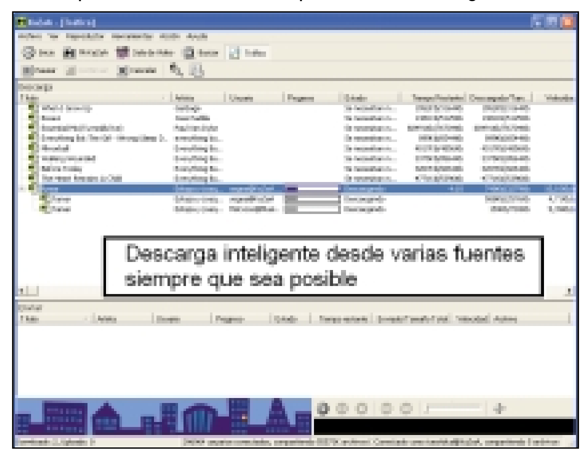
Normalmente el número máximo de resultados de una búsqueda se establece en 50. La razón de la elección de esta cifra relativamente pequeña es que el objetivo de KaZaA es encontrar los resultados más relevantes. Cuando realizamos una búsqueda, los resultados obtenidos se agruparán, de forma que el mismo archivo únicamente aparece una vez, siendo más fácil localizar los archivos. No obstante, podemos aumen-



tar este límite hasta un máximo de 100 resultados a través del menú *Herramientas/Opciones*, bajo la pestaña *Avanzado*. Asimismo, podremos encontrar más archivos del mismo artista o álbum si, tras haber realizado la búsqueda inicial del archivo, hacemos clic con el botón derecho sobre el mismo y en el menú contextual seleccionamos la opción *Buscar más de éste* y luego en las opciones *Album*, *Artista seleccionado* o *Usuario*.

Descarga de archivos

Para descargar un archivo, haremos doble clic sobre el elemento en la página de resultados de la búsqueda. Automáticamente se iniciará el motor de descarga inteligente, que tratará de encontrar el mejor camino para descargar el archivo, así como encontrar la/s fuente/s más rápida/s. Desde la vista *Tráfico* podremos monitorear el proceso de descarga de datos.

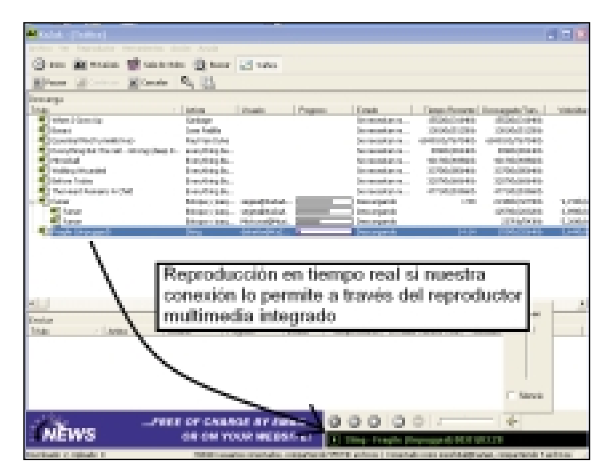


En caso de que sea posible, los archivos serán descargados de múltiples fuentes simultáneamente, acelerando de esta manera la descarga y pudiendo ser resumida si se rompe por algún motivo, como por ejemplo la desconexión del ordenador remoto desde donde descargábamos el archivo. Para ello, recomendamos descargar al mismo tiempo una cantidad razonable de archivos de acuerdo con la calidad de nuestra conexión y hacerlo siempre que sea posible desde máquinas con conexiones de alta velocidad.
El siguiente cuadro indica la velocidad estimada a la que regularmente podremos descargar los archivos desde KaZaA, dependiendo del tipo de conexión con la que contemos:

	Módem, 56 Kbps	**Cable, 512 Kbps**	**T1, 2 Mbps**
Imagen, 200 Kbytes	40 segundos	2 segundos	2 segundos
Tema musical, 4 Mbytes	13 min, 30 seg.	1 minuto	15 segundos
Película completa, 400 Mbytes	22 horas	1 hora, 45 min.	25 minutos
Video clip de 5 minutos, 20 Mbytes	1 hora	6 minutos	2 minutos
Novela de 200 páginas, 1 Mbyte	4 minutos	15 segundos	4 segundos

Durante la descarga

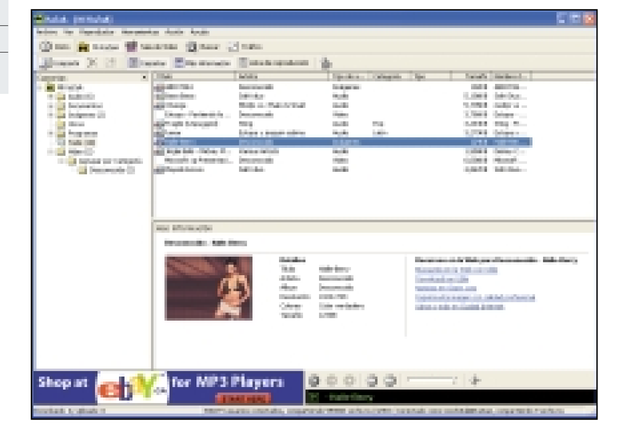
Una de las opciones disponibles en KaZaA es la de reproducir archivos mp3 en tiempo real al mismo tiempo que están siendo descargados, gracias al reproductor integrado que encontraremos en la parte inferior derecha de la ventana de *Búsqueda* o *Tráfico*. También destacamos que podemos dejar los archivos que nos queramos bajar «en cola de espera» pulsando con el botón derecho del ratón sobre el archivo dentro de la vista *Tráfico* y seleccionando en el menú contextual la opción *Detener descarga*. De esta forma se irán descargando



consecutivamente. Y si, por cualquier motivo, nuestra conexión o la del usuario que tiene en su disco duro el MP3 que queremos se interrumpe, KaZaA guardará la información para reiniciar la descarga automáticamente cuando sea posible. KaZaA También permite el envío de mensajes instantáneos entre usuarios, si bien no existe la figura de un sitio donde poder compartir conversaciones en grupo. Para ello, haremos clic con el botón derecho del ratón sobre el archivo que estamos descargando, y seleccionaremos la opción *Enviar mensaje al usuario* para hablar con su dueño. De la misma manera, en la pestaña *Mensajes* dentro del menú *Herramientas/Opciones* podemos evitar la recepción de mensajes por parte del resto de usuarios, marcando la casilla *Ignorar todos los mensajes entrantes* o ignorar los mensajes de algunos usuarios concretos, para lo que será necesario introducir su nombre dentro de la lista de *Ignorados*.

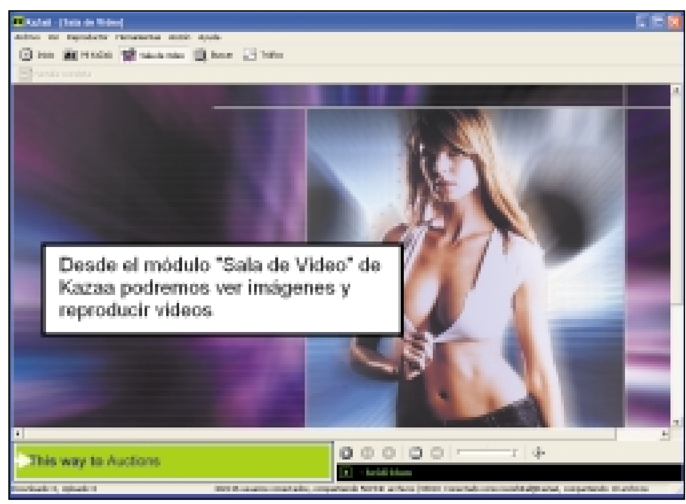
Mi KaZaA

Mi KaZaA organiza automáticamente todos los archivos descargados y aquellos que vayamos a compartir con el resto de miembros del servicio. Éstos se ordenarán automáticamente de acuerdo al tipo de archivo multimedia, artista, categoría, etc. Desde Mi KaZaA podremos calificar los archivos o editar detalles a los que tendrán acceso el resto de usuarios de KaZaA, lo que contribuirá a la selección que puedan hacer de los mismos, eliminar archivos de nuestro duro (mediante su selección y pulsando sobre la tecla *Suprimir*), compartir o dejar de compartir archivos. Pero lo más importante de *Mi KaZaA* es que podremos reproducir archivos de audio y crear nuestras propias compilaciones de archivos de audio en la *Lista de reproducción*. Desde *Inicio* podremos visualizar documentos de Word, PDF de Acrobat, hojas de cálculo de Excel, etc.



Sala de vídeo

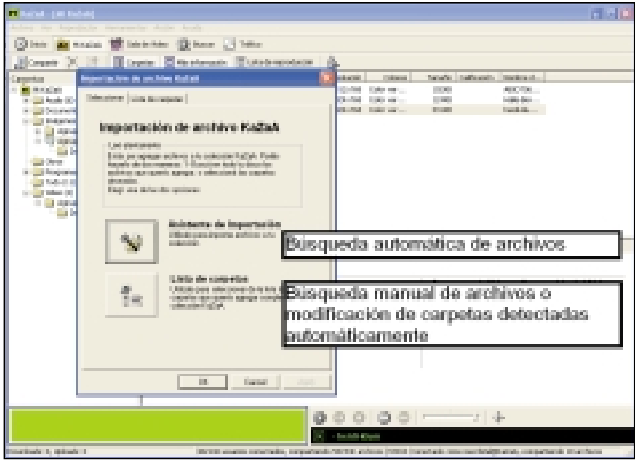
La sala de vídeo es un módulo de KaZaA donde podremos ver imágenes y vídeos. En el caso de los vídeos, podremos visualizarlos a pantalla completa pulsando sobre el icono



existente en la *Barra de tareas*, y en el modo pantalla completa pulsaremos con el botón derecho en cualquier parte de la ventana del vídeo para desmarcar la opción *Pantalla completa* de forma que volvamos a la ventana principal del programa.

Cómo compartir archivos

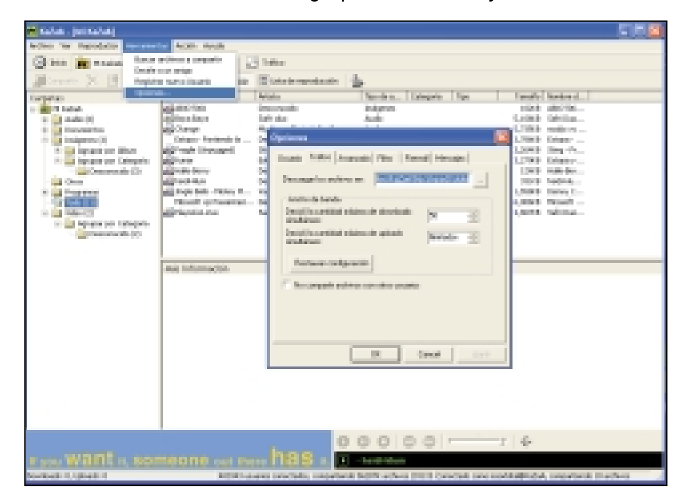
Si hemos decidido compartir los archivos en nuestro disco



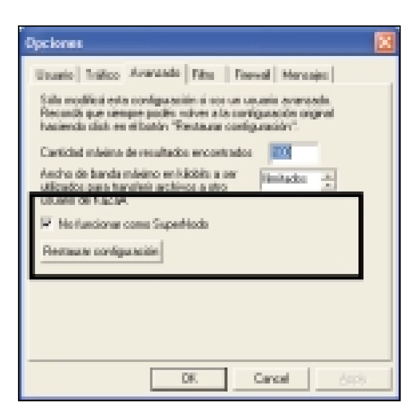
duro al resto de usuarios de KaZaA, podemos hacerlo de dos maneras, dejando a KaZaA que escanee los discos duros en busca de carpetas que contengan archivos multimedia y seleccionando después cuáles de ellas queremos compartir o hacerlo directamente de forma manual. En el primer caso, dentro del menú *Herramientas/Buscar archivos a compartir* pulsaremos sobre el botón *Asistente de Importación*. El segundo método consiste en seleccionar carpetas enteras que queramos compartir, como por ejemplo una carpeta que tenga un disco en formato MP3. Para hacerlo, dentro del menú *Herramientas/Buscar archivos a compartir* pulsaremos el botón *Lista de carpetas*, donde veremos una lista de las carpetas que forman parte de nuestro sistema, que podremos expandir haciendo clic sobre el signo «+» y marcando la casilla de verificación. Observaremos que los contenidos de las subcarpetas existentes bajo una carpeta compartida también serán compartidos. De la misma forma, podemos compartir archivos simplemente copiándolos a la carpeta de archivos compartidos.

Evitar la compartición de archivos

Dentro del menú *Herramientas/Opciones* de KaZaA, bajo la pestaña *Tráfico,* podemos determinar la carpeta donde se almacenarán los archivos descargados de KaZaA, por defecto *\KaZaA\My Shared Folder*. Bajo el apartado *Ancho de banda*, estableceremos el número máximo de descargas y *uploads* que podremos mantener simultáneamente. En cualquier caso, tendremos que asegurarnos de no compartir aquellos archivos que queramos mantener en privado o aquellos protegidos por la ley. En ese caso, existen tres formas de dejar de compartir archivos; dentro de Mi KaZaA, haciendo clic con el botón derecho del ratón sobre el archivo concreto o grupo de archivos y seleccionando la



opción *Dejar de Compartir* que aparecerá en el menú contextual. Podremos dejar de compartir una carpeta completa seleccionando *Herramientas/Buscar archivos a compartir* y desmarcando la casilla de verificación de una carpeta que ya no queramos compartir. También es posible desactivar por completo la compartición de archivos con otros usuarios, marcando la casilla «No compartir archivos con otros usuarios», si bien vulneraremos los principios de este tipo de programas. Para saber si estamos o no compartiendo un archivo, observaremos si bajo el icono del archivo aparece una mano, en cuyo caso se tratará de un archivo compartido.



La opción SuperNodo

Dentro del menú *Herramientas/Opciones* de KaZaA, bajo la pestaña *Avanzado,* encontramos una críptica casilla llamada «No funcionar como SuperNodo». Debido al diseño auto-distribuido de la red de KaZaA, no existe como en Napster la figura de un servidor central encargado de gestionar las búsquedas de archivos de todos los usuarios. En su lugar, todos los usuarios de KaZaA hacen de nodos repetidores de las búsquedas, distribuyendo de esta

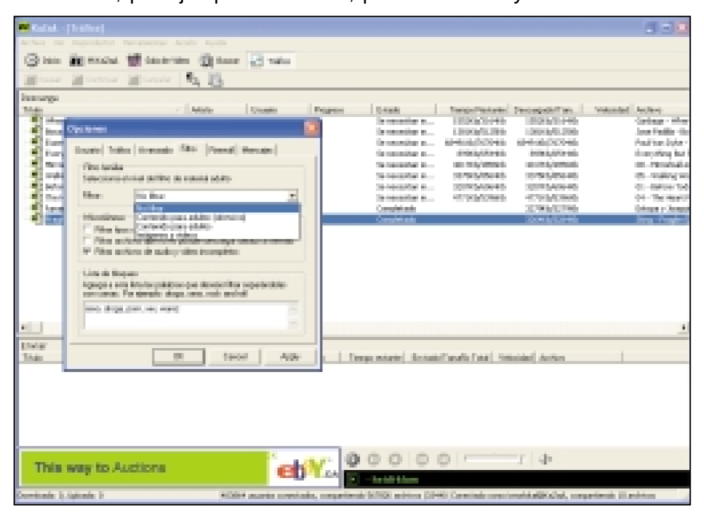
forma la carga de datos que una búsqueda en redes tan grandes comporta. Sin embargo, los usuarios que disponen de conexiones más lentas (por ejemplo a través de módem) no podrán sostener este ritmo de tráfico, por lo que podrán configurar su cliente de KaZaA para que no actúe como repetidor en estas funciones. En cambio, los usuarios que cuentan con conexiones más rápidas y ordenadores más potentes, deberán funcionar como SuperNodos.

Cancelar los uploads

Cuando se cancela el envío de un archivo, éste termina. Esto resulta especialmente útil en conexiones a través de módem, donde las peticiones de descarga de otros usuarios pueden reducir nuestra propia capacidad para obtener archivos. Sin embargo, es necesario ser precavido en el uso de este comando, ya que la cancelación del envío de un fichero no es nada agradable para quien está haciendo la descarga de nuestro archivo. Esta persona puede haber estado haciendo la descarga del archivo por varios minutos y el hecho de cancelarla implica que se quede sin ese archivo. Sin embargo, para cancelar el envío de datos, seleccionaremos el archivo dentro de la lista de envíos bajo la pestaña *Tráfico* y con el botón derecho del ratón seleccionaremos la opción *Cancelar Enviar*.

Filtros

KaZaA incluye unos filtros que permiten ajustar el nivel de seguridad respecto al contenido de los archivos que podemos descargar. Podemos catalogar dos tipos de filtros. El *filtro Familiar*, relacionado con el nivel de contenido para adultos que podremos descargar, cuyas opciones son: *Sin filtro, offensive adult content, adult content, images and videos* y luego unos filtros extra, como son los archivos que potencialmente puedan contener virus, archivos que no puedan ser descargados por la existencia de cortafuegos o canciones y archivos de vídeo defectuosos. No todos los archivos pueden contener virus o troyanos. Los archivos de música, vídeo y fotos son, generalmente, seguros. En este grupo figuran aquellos con extensiones «.mp3», «.wav», «.mpg», «.avi», «.mov»,«.bmp» y «.jpg». Los documentos PDF («.pdf») y los archivos de texto («.txt») son igualmente seguros. Pero deberemos extremar la precaución con los ejecutables («.exe»), documentos de Microsoft Word y plantillas Excel, por ejemplo. Asimismo, podemos crear y man-





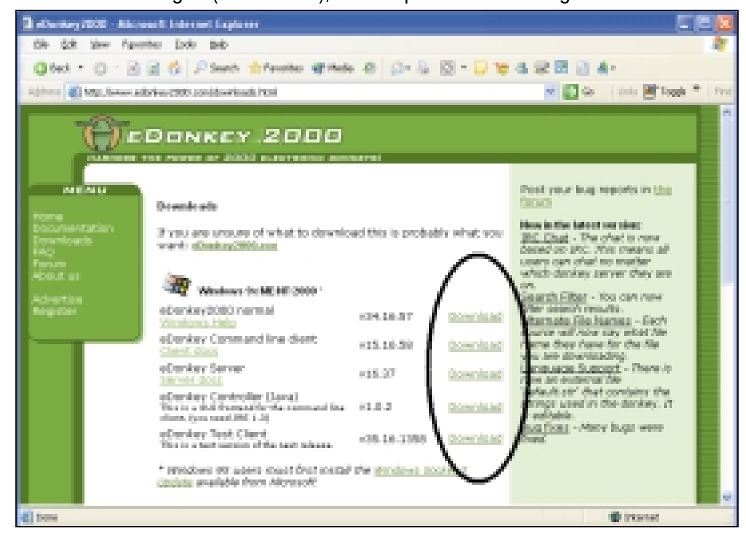
tener una lista de palabras cuya presencia en el nombre de un archivo evitará que puedan ser descargadas. Estas palabras han de estar separadas por una coma, por ejemplo: «sexo, drogas, warez».

eDonkey 2000

Se ha erigido como una de las alternativas más serias y versátiles a Napster, convirtiéndose en uno de los programas de intercambio de archivos más populares del mercado. Está basado en el protocolo MFTP (*Multisource File Transfer Protocol*) y permite transferir todo tipo de archivos. Además soporta el uso de *skins*, incluyendo dentro del paquete inicial las interfaces *clásica* y *reddonkey*, a las que podremos añadir las que vayamos creando con sólo seguir las instrucciones contenidas en la página *www.edonkey2000.com/ui.html*.

Descarga e instalación

Desde la página web principal de eDonkey, en *www.edonkey2000.com*, encontramos el enlace a la sección de descargas (*Downloads*), donde podemos descargar una versión del



cliente compatible con Windows 9x/Me/NT/2000/XP, otra para Linux y una última para Mac OS X.

Una vez instalado el programa, bajo el directorio *\ARCHIVOS DE PROGRAMA\EDONKEY* encontraremos una serie de archivos:

«known.met» Este archivo almacena la identificación de los archivos y segmentos de archivo que hemos descargado anteriormente, De esta manera, eDonkey no ha de volver a identificar los archivos de los directorios compartidos cada vez que se inicia.

«pref.met» Almacena las preferencias de configuración del programa: nombre de usuario, velocidad de descarga…

«shared.dat» Contiene la lista de directorios marcados para compartir con el resto de usuarios. Eliminando este archivo únicamente compartiremos el contenido del directorio *\ARCHIVOS DE PROGRAMA\EDONKEY\INCOMING*.

«server.met» Lista los servidores conocidos.

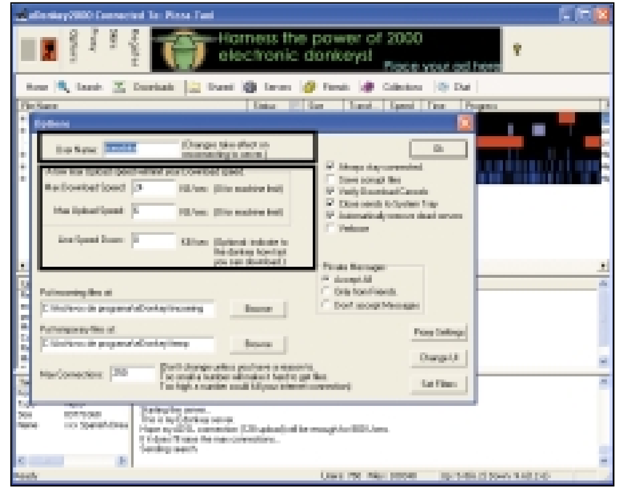
«friends.met» Lista los usuarios que hemos marcado como amigos.

«layout.dat» Determina el tamaño de las ventanas y las cabeceras de columna de la aplicación.

«Default.str» Contiene las cadenas utilizadas dentro del programa y es editable, por lo que podemos modificarlo para transformar en español los diálogos del programa.

Registro y configuración inicial

El programa eDonkey no precisa un registro si entendemos como tal la necesidad de crear una cuenta de usuario con una contraseña que verifique su identidad. Sin embargo, sí debemos introducir un nombre único de usuario, dentro del menú

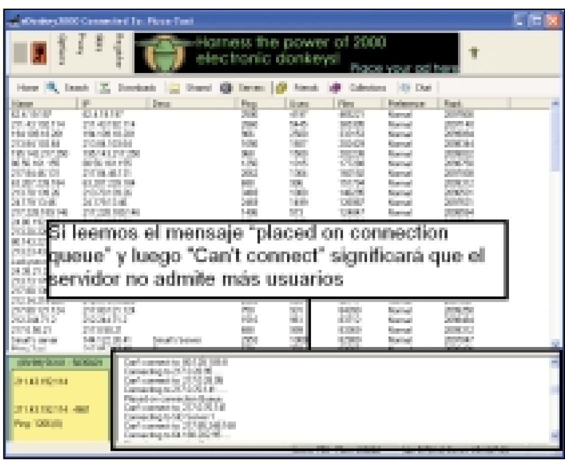


Options (opciones) en el cuadro *User name* la primera vez que iniciemos el programa, ya que de lo contrario se nos asignará un nombre aleatorio. También definiremos las velocidades máximas de descarga y subida de archivos, de acuerdo con la potencia de nuestra conexión. No obstante, si especificamos un valor demasiado bajo para la velocidad de subida de archivos, se verá limitada la velocidad de descarga. Los valores mínimos de subida son:

Valor mínimo de subida	Valor máximo de bajada
0 (ilimitado)	0 (ilimitado)
1	3
2	6
3	9
4	12
5	20
6	24
7	28
8	32
9	36
10 o más	ilimitado

Si no podemos conectarnos a un servidor eDonkey

Es posible que el servidor al que estamos intentando conectar no admita más usuarios. Si dentro de la barra de estado situada en la parte inferior de la pestaña *Server* (servidor) leemos el mensaje *«placed on connection queue»* y luego *«Can't connect»*, significará que el servidor no admite más usuarios. Sin embargo, podremos intentar conectar a cualquier otro servidor. Independientemente de esto, cuando iniciemos el programa, inmediatamente y sin necesidad de conectarnos a ningún servidor, buscará usuarios sobre los que poder descargar las partes restantes de los archivos que tengamos pendientes y el resto de usuarios podrán acceder a los archivos que nosotros



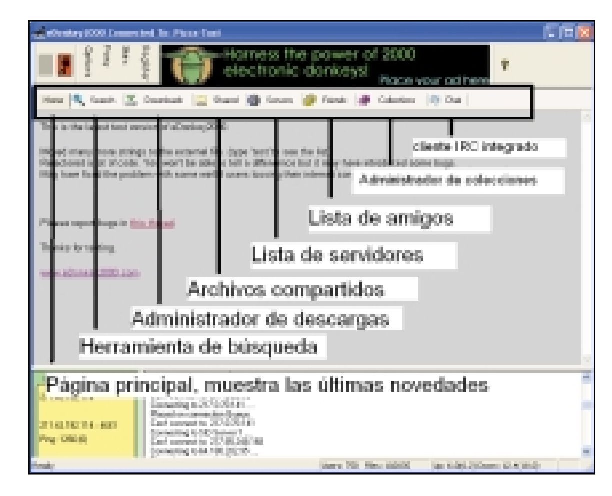
estemos compartiendo para descargarlas en su propio ordenador. Una vez estemos conectados a un servidor, para evitar perder la conexión dentro del menú *Options* marcaremos la casilla existente en el campo *Always stay connected*.

Puertos que utilice eDonkey

Para asegurarnos el correcto funcionamiento de eDonkey, nos aseguraremos que los puertos que la aplicación utiliza no estén bloqueados por ningún *router, firewall* o nuestro ISP. Estos puertos son:
Puerto TCP 4661 para conectar al servidor.
Puerto TCP 4662 para conectar a otros clientes.
Puerto UDP 4665 para enviar mensajes a otros servidores diferentes del que estamos conectado

Una vista rápida a la interfaz de usuario

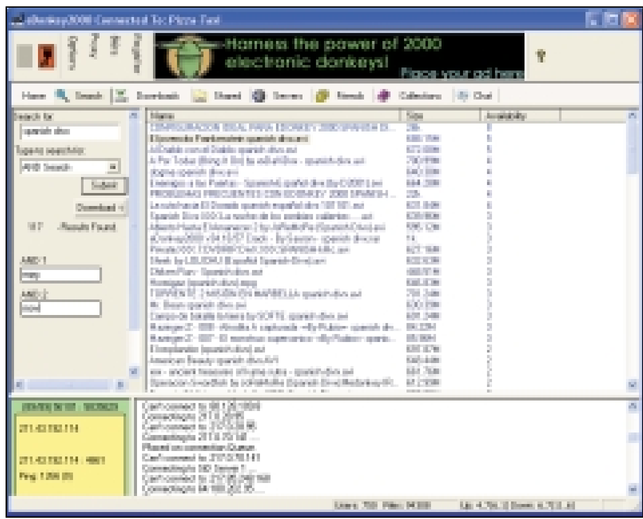
-**Search**: desde aquí buscaremos archivos que estén compartidos por el resto de usuarios.
-**Downloads**: desde aquí veremos el estado actual de nuestras descargas y *uploads*.
-**Shared**: escogeremos qué archivos compartiremos con el resto de usuarios.
-**Servers**: la lista de servidores disponibles.
-**Friends**: nos permite seguir la pista de usuarios con los que compartamos intereses comunes.
-**Options**: las opciones de configuración del cliente para que se comporte como deseamos.



-**Collections**: nos indicarán los archivos de compilaciones (archivos multimedia formados por varios archivos).
-**Chat**: un área donde podremos hablar con el resto de usuarios de la comunidad.

Búsqueda de archivos, al detalle

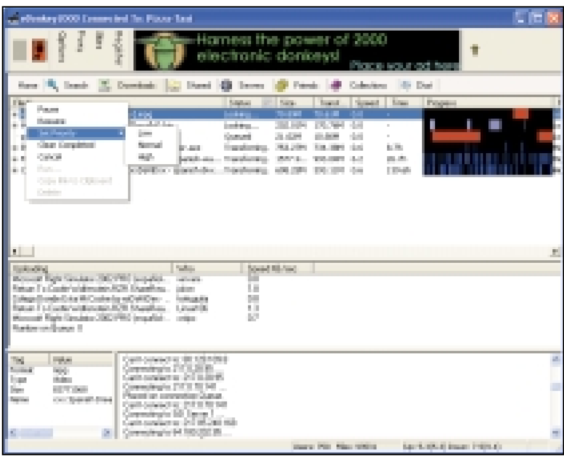
Debido a que el programa no dispone de servidores centrales y su filosofía de funcionamiento es similar a la de Gnutella, las búsquedas se realizarán sobre el resto de máquinas que forman la red. Por esta razón, al conectarnos a un servidor, automáticamente el cliente eDonkey indicará los archivos que compartiremos al servidor, de forma que cada servidor mantendrá una lista de todos los archivos compartidos de todos los clientes conectados. Así, cuando un cliente envía una petición de búsqueda a su servidor, éste no consultará en cada uno de los clientes que tiene conectados, sino en la lista de archivos compartidos por los clientes que tiene en su poder. Para buscar un archivo, dentro de la pestaña *Search* introduciremos uno o varios términos en la caja *Search for:* y, opcionalmente, bajo *Type to search for:* el tipo de archivo que queremos descargar: audio, vídeo, imágenes, programas, documentos, colecciones, usuarios, búsqueda de MP3 o de cualquier tipo, así como



búsquedas extendidas de tipo *AND* y *OR* para retornar archivos que contengan ambas o una de las dos palabras; así como el tamaño y formato de éste. Tras introducir estos parámetros, pulsaremos sobre el botón *Submit* para efectuar la búsqueda en el servidor al que estamos conectados o sobre *Extend Search* tantas veces como deseemos para extender nuestra búsqueda a los servidores cercanos al que estemos conectados.

Descarga de archivos

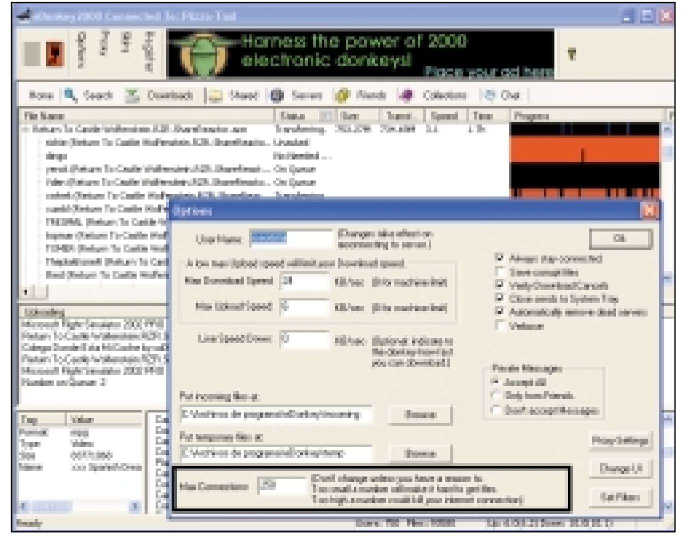
Tras localizar el archivo dentro del resultado de la búsqueda, haremos doble clic sobre el mismo para comenzar la descarga. Desde la pestaña *Downloads* podemos monitorizar el estado de las descargas. Con el botón derecho del ratón haremos:
-*Parar* la descarga.
-*Resumir* (sólo si antes habíamos parado) la descarga, lo que provocará el inicio de la descarga si la fuente del archivo está disponible.
-Establecer la *Prioridad* de la descarga, que afectará al orden en que los archivos se verán cuando estén en la cola de descargas.



-*Limpiar completos*, que eliminará de la cola de descargas los archivos que hayan sido correctamente transferidos.
-*Cancelar* una transferencia de archivos.

Descarga de múltiples fuentes

eDonkey permite descargar simultáneamente un mismo archivo desde diversos usuarios, incluso cuando estos otros usuarios estén todavía descargándose este mismo archivo. Sin embargo, si el archivo está muy solicitado, en su estado aparecerá *«Remotely Queued»*. Esto será porque la gente que tiene el archivo que queremos ya lo está sirviendo a otros usuarios. En ese caso, la descarga comenzará cuando algún



usuario deje libre un *slot* de descarga. Dentro del menú *Options*, podremos definir el número máximo de conexiones a otros usuarios que nuestro cliente podrá establecer para intentar descargar un archivo. Debemos tener en cuenta que un número muy pequeño limitará las posibilidades de descarga del mismo, así como un número muy grande podrá llegar a «matar» nuestra conexión de Internet.

Qué hacer cuando una descarga está corrupta

En el cuadro de estado de la descarga, en ocasiones podemos ver el mensaje *«Corruption found in* nombrearchivo at part X». Esto significará que un segmento parcial de 9 Mbytes del

archivo no tiene los mismos bytes que la copia original que nos fue enviada. Esto no implica que el archivo final obtenido vaya a quedar inutilizable, pero sí que esa parte de la descarga será eliminada y volverá a ser descargada.

Finalizar las descargas

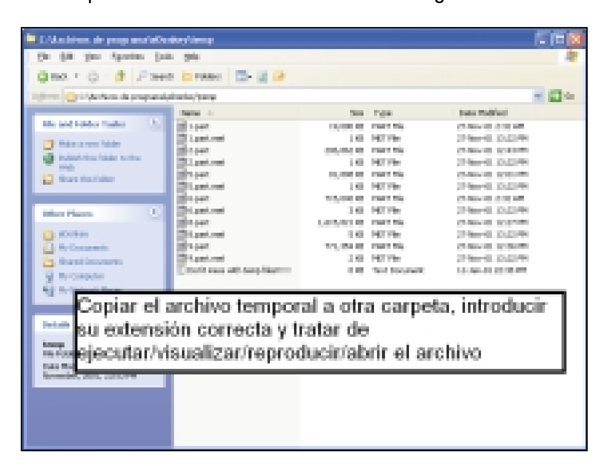
Un punto en el que eDonkey debe mejorar es a la hora de finalizar las descargas. De hecho, con archivos de gran tamaño, muchas veces el archivo descargado se mostrará en la ventana principal del programa con mayor tamaño que el original. Esto es debido a que, cuando descargamos un archivo de más de una fuente, el programa pedirá un segmento de 9 Mbytes del archivo a cada uno. Si una fuente no envía la información que pedimos cuando este es el último segmento restante, el programa preguntará a otra fuente que le envíen este segmento. Esto puede causar que algunos bytes sean enviados dos veces, provocando que el archivo transferido sea mayor que en tamaño que el original. El problema se agudiza en conexiones lentas y con archivos populares.

Espacio en disco insuficiente

Ya que las descargas en eDonkey no siempre comienzan con el principio y acaban con el final del archivo, se necesita suficiente espacio disponible en disco para que el cliente escriba en cualquier segmento del archivo. Por ello, eDonkey verifica para cada descarga activa que exista tamaño suficiente en el disco para que pueda aumentar su tamaño hasta su tamaño final. Si una descarga activa cambia a inactiva (parada o espacio en disco insuficiente), el espacio en disco no utilizado por este archivo quedará sin reservar y otras descargas que previamente tuvieran el estado «espacio insuficiente en disco» posiblemente podrán reiniciarse. Si queremos que un archivo particular cuyo estado sea «espacio insuficiente en disco» comience la descarga, tendremos que liberar la cantidad de espacio en disco necesaria (puede pasar un tiempo hasta que el cliente se dé cuenta de que hemos liberado espacio) o establecer la prioridad de descarga del archivo como alta (*High*) y pasar a otra descarga activa.

¿Puedo abrir/ver/utilizar archivos parciales?

No es una buena idea, ya que eDonkey no incluye un reproductor integrado, y la filosofía de descarga de archivos provoca que no necesariamente se descarguen de forma

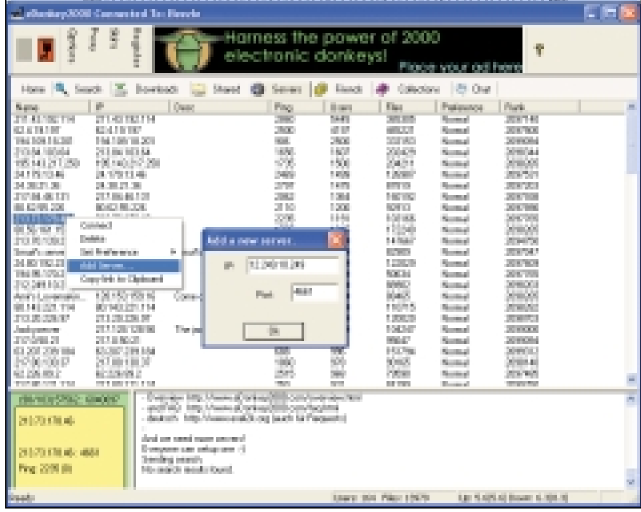


Copiar el archivo temporal a otra carpeta, introducir su extensión correcta y tratar de ejecutar/visualizar/reproducir/abrir el archivo

secuencial de principio a fin, algo necesario en muchos de los formatos de archivo para poder ser visualizados/ejecutados. En cualquier caso, si no tenemos intención de finalizar la descarga o queremos comprobar el contenido de un archivo, copiaremos al escritorio el archivo «.part» de la carpeta *\ARCHIVOS DE PROGRAMA\EDONKEY\TEMP* que corresponda con el tamaño final del archivo, y modificaremos su extensión a la original.

Servidores

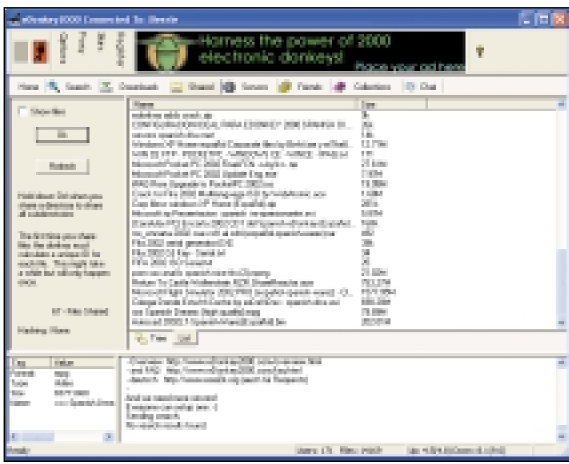
Los servidores aparecerán automáticamente en la lista de servidores a medida que estén disponibles públicamente para los usuarios de eDonkey. Debido a que cualquier ordenador puede convertirse en un servidor eDonkey, esta lista es dinámica, de forma que va aumentando a medida que se



añaden a la red nuevos servidores. Dentro del menú *Options* podremos definir si los servidores «muertos» (aquellos que se hayan desconectado de la red) permanecerán en la lista de servidores disponibles o automáticamente serán eliminados, marcando la casilla *Automatically remove dead servers*. Para añadir un servidor, pulsaremos con el botón derecho del ratón sobre la lista y seleccionaremos la opción *Add A New Server*. Desde aquí también podremos definir la *prioridad* de un servidor. Esto afectará al orden en que el cliente intentará reconectar a la comunidad cuando se desconecte. Haciendo doble clic sobre un servidor intentaremos conectarnos a él y, finalmente, si un servidor parece imposible de conectar o no es operativo, podremos eliminarlo desde el mismo menú contextual con la opción *Delete*.

Compartir o no compartir, y la mejor forma de hacerlo

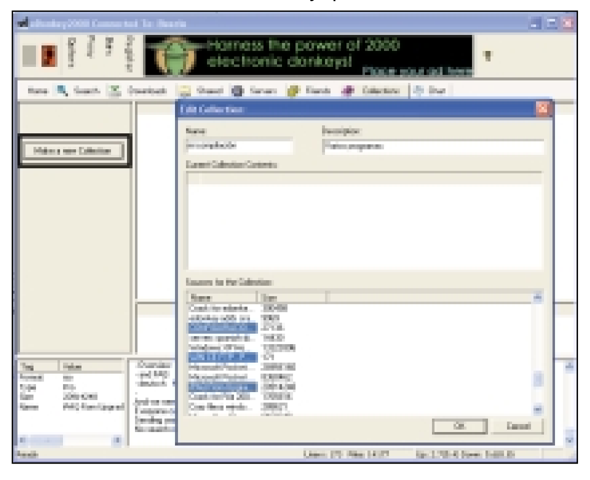
Desde la pestaña *Shared* podremos definir bajo *Tree* (árbol) las carpetas cuyo contenido compartiremos con el resto de usuarios del servicio eDonkey, así como concretamente una lista (*List*) de los archivos que tenemos compartidos. Para compartir el contenido de nuevas carpetas, haremos clic sobre el cuadro de la carpeta para añadir la marca de verificación. Al pulsar sobre *Ok*, el programa verificará los archivos compartidos, dándoles un identificador único. De esta forma, si un archivo encontrado en diferentes ordenadores queda determinado por el identificador como el mismo



archivo, se podrán descargar partes de diferentes ordenadores al mismo tiempo para acelerar el proceso de descarga, y poder resumir la descarga del archivo de otra fuente de la que originalmente provenía.

Collections

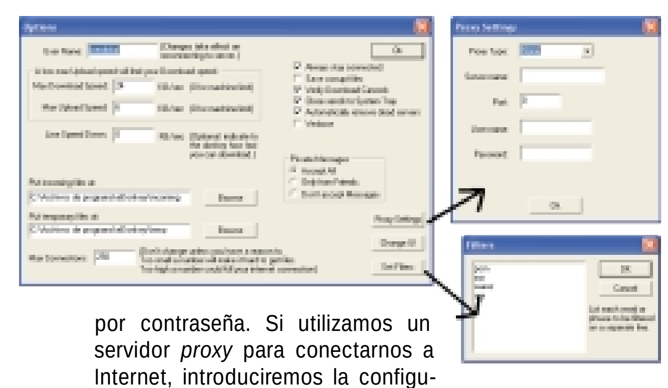
Las *collections* (colecciones) son un método para organizar los archivos que normalmente se encuentran divididos en varios ficheros más pequeños. Si por ejemplo queremos compartir un álbum de música en eDonkey, podemos crear una colec-



ción que incluya todas las canciones del álbum, conjuntamente con archivos gráficos de las carátulas de portada y contraportada. Esta es una forma de asegurarnos que el resto de usuarios podrán obtener el álbum completo. Para crear una colección, pulsaremos sobre el botón *Make a new collection* dentro de la pestaña *Collections* y, tras darle un nombre y una descripción, seleccionaremos los archivos que formarán parte de él. De esta forma, cuando alguien descargue nuestra colección recibirá todos los archivos asociados a ella o podrá determinar descargar únicamente las partes que quiera de esta colección. Únicamente podremos crear colecciones con archivos de carpetas que tengamos compartidas en eDonkey.

Filtros y conexión a través de Proxy

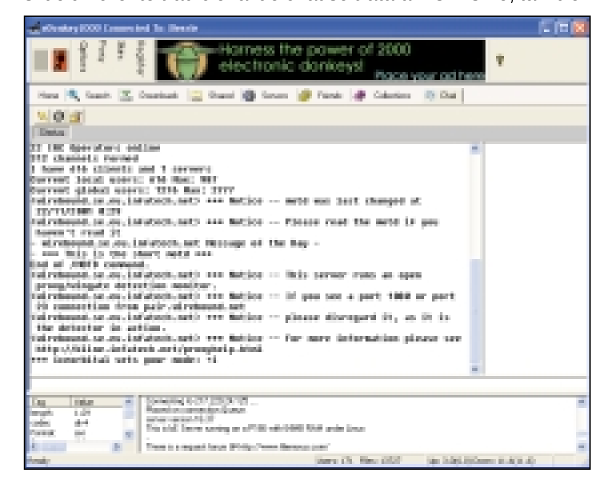
Bajo el menú *Options* encontraremos un botón *Set filters* en el que podremos definir palabras concretas o frase enteras para restringir los resultados de las búsquedas, si bien esta característica no está como en otros programas protegida



por contraseña. Si utilizamos un servidor *proxy* para conectarnos a Internet, introduciremos la configuración del mismo (tipo de servidor, dirección, puerto) y, si es necesario, nombre de usuario y contraseña, pulsando sobre el botón *Proxy* en la barra de herramientas de la ventana principal del programa

Mensajes

eDonkey incorpora funciones de chat a través de la red IRC, de forma que todos los usuarios podrán conectarse entre sí para charlar con independencia del servidor al que se conecten. Para ello pulsaremos sobre la pestaña *Chat* y luego sobre el botón *Conectar*. Una vez conectado, seleccionaremos los canales en los que participaremos y haremos funcionar el programa como si de un cliente tradicional de chat se tratara. Asimismo, también



podremos recibir y enviar mensajes privados a otro usuarios haciendo clic con el botón derecho del ratón sobre el usuario al que queramos consultar y seleccionando la opción *Send message*. Desde el menú *Options* del programa personalizaremos su comportamiento frente a este tipo de mensajes, desde aceptar todos los mensajes (*Accept All*), aceptar mensajes únicamente de los usuarios establecidos como amigos dentro de la pestaña *Friends* (*Only from friends*) o no aceptar ningún tipo de mensaje privado (*Don't accept Messages*).

los colores de la barra de progreso

Negro: los segmentos del archivo que hemos descargado.
Rojo: partes que todavía no se han encontrado en la red eDonkey.
Gris: partes que estamos intentando descargar.
Tonalidades de azul: cuanto más azul, más usuarios tienen ese segmento del archivo.

Otras alternativas a Napster

AGStreme
www.ractive.ch/gpl/JAGS.html
Sustituto de Audiogalaxy Satellite mucho más completo que utiliza su misma red. Incluye un editor de información ID3 y reproductor, base de datos de música, múltiples búsquedas simultáneas, nuevo nombre, etc.
AudioGnome *www.audiognome.com*
Programa muy completo con filtros para encontrar archivos con mayor facilidad, chat con los usuarios (incluso a través de IRC), centenares de servidores y completa red de usuarios,
Badblue *http://badblue.com*
Funciona a través de una interfaz web a través del navegador, con opciones de IRC.
BlackWidow *www.communeweb.com*
Soporta los protocolos Gnutella y Opennap, reproductor MP3, visualizador de imágenes, búsqueda por categorías, mensajería interpersonal y comunicaciones encriptadas entre usuarios.
Blubster *www.blubster.com*
Bastante rápido al mostrar resultados, con resumen de descargas desde usuarios diferentes, chats de voz y reproductor multimedia integrado.
BodeTella *www.felmlee.com/bodetella*
Sencillo clon de Gnutella con resumen de descargas.
BuddyShare *www.buddyshare.org*
Descarga todo tipo de archivos de vídeo, imágenes, MP3…, con resumen de descargas y chat.
Digisecret *www.tamos.com/products/digisecret* Emplea un algoritmo de encriptación al compartir los archivos.
Direct Connect *www.neo-modus.com*
Posibilidad de compartir cualquier tipo de archivos sin restricciones ni filtros en una comunidad creada, controlada y administrada por los propios usuarios. Interfaz similar a la del Explorador de Windows. Chats público y privado.
eBlvd Premium File Sharing
www.eblvd.com Funciona como un navegador, conectando directamente con otros usuarios sin necesidad de directorios, cuellos de botella o registros de acceso (2 dólares al mes).
ELF *www.projectelf.com* Su principal objetivo es mantener el anonimato del usuario y de sus transferencias de datos. Tiene descargas simultáneas y limitación de ancho de banda.
FileSpread *www.secureup.com* Como novedad incluye la posibilidad de abrir sesiones de control remoto.
File Rogue *www.filerogue.com*
Te permite el intercambio sin restricciones de ficheros. El intercambio se realiza de usuario a usuario. Cada usuario comparte unos ficheros que son incluidos en un catálogo global.
Flipr *www.flipr.com*
Toda la música que se puede intercambiar son archivos 100% cedidos por los autores y sellos discográficos. Música alternativa, y 100% legal, incluyendo información detallada de cada una de las canciones.
Freenet *http://freenet.sourceforge.net*
Funciona como la World Wide Web pero con algunas importantes diferencias. La información en Freenet no está almacenada en lugares fijos. Es una red descentralizada que incluye técnicas de *routing* y *mirroring*. Se dice de ella que es una red más libre puesto que se puede publicar lo que se quiera sin peligro de que se descubra el origen de la información.
Instant Net Files *www.zedplace.com*
Interfaz en forma de tablón de anuncios. Requiere cuentas FTP con acceso de escritura para compartir archivos, si bien las direcciones http se pueden utilizar para leer mensajes o descargar archivos.
I-Share
http://cis.tzo.com/software/gjsoftware
Descarga de gran cantidad de MP3, DVD, *ebooks* y otros archivos. Conexión a servidores rápidos y chat.
JungleMonkey *www.junglemonkey.net*
Se aplica también la idea de la distribución de máquinas a las que nos conectamos mediante canales, algo así como lo que ocurre en un programa de chateo.
Konspire.*http//konspire.sourceforge.net*
Presenta la peculiaridad de estar programado en Java, lo que lo independiza de la plataforma.
Mojo Nation *www.mojonation.net*
Este programa no sólo nos conecta a una red protegida criptográficamente, sino que hace uso de nuestro disco duro y nuestros ciclos de reloj (del procesador, en cristalino) para poder ejecutar aplicaciones complejas o almacenar contenidos extra.
MP3 Board *www.mp3board.com*
MP3Board no tiene un software cliente ni para las búsquedas, ni para las descargas, ni es necesario el registro. Es un buscador de MP3 en los protocolos http y ftp, así como en la red Gnutella.
NapAmp *http://napamp.sourceforge.net*
Una extensión del reproductor Winamp que le permite buscar y descargar canciones desde redes OpenNap.
Newtella *www.newtella.com*
Clon de Napster que hace uso de la tecnología de Gnutella (todos los usuarios son servidores y clientes) para encontrar y descargar MP3. Incluye opciones de seguridad.
PicXchange *www.grasshopper.com*
Es una aplicación *peer-to-peer* especialmente para compartir imágenes con los amigos, que incluye chat, generación automática de vistas en miniatura y transferencias seguras de imágenes.
Riffshare *www.riffshare.com*
Riffshare convierte una LAN en una red de jukebox digitales. Es perfecto para intercambiar MP3; el único requisito es que tu ordenador forme parte de una LAN.
Smirck *www.smirck.com*
Clon de Napster que únicamente permite descargar archivos MP3.
SongSpy *http://www.songspy.com*
Interfaz muy sencillo de usar y altamente configurable. Su filosofía es algo así como «Da y coge», ya que no permite interrumpir «uploads». Este programa de intercambio de ficheros incluso premia a sus usuarios más activos. Incluye lista de contactos, velocidades de las líneas de los usuarios y gestor/reproductor de canciones.
Swapoo *www.swapoo.com*
Aquí principalmente lo que se intercambian son juegos. El intercambio es de Usuario a Usuario (p2p).
Swaptor *www.swaptor.com*
Programa limitado en sus funciones que nos permitirá intercambiar todo tipo de ficheros, crear grupos de usuarios y chatear con ellos.
Wanafile *www.wanafile.com*
Incluye un potente motor de búsqueda de imágenes, documentos, música, vídeos, aplicaciones y otros tipos de archivos en Internet.
Yaga Share *www.yaga.com*
Su manejo es similar al de Audiogalaxy, haciendo uso de un programa satélite para gestionar las descargas de ficheros obtenidas a través de una búsqueda en su página web. Permite descargar MP3, MPEG, AVI o ficheros de imagen.



Streaming de vídeo

Descubre el mundo de la radio y el vídeo a través de Internet / CD

La decadencia del mundo de las ondas ha comenzado. La implantación de la tecnología de banda ancha en nuestro país acerca a todos los usuarios las enormes posibilidades de la radio y el vídeo a través de Internet. Inevitablemente, la era de la aldea global ha llegado. A pesar de que a estas alturas resulta difícil asombrarse ante las barreras que la tecnología derriba cada día, no es posible quedarse impasible al descubrir todo lo que Internet pone al alcance de nuestras manos. Por supuesto, esto no es nuevo. Todo aquel que conozca en mayor o menor medida la Red es consciente de lo que representa. Pero esta circunstancia no evita cierta perplejidad ante la posibilidad de escuchar la radio Bloomberg WBBR de Nueva York o disfrutar de los mejores vídeos emitidos por la MTV, todo ello en directo y con la mejor calidad. Como es obvio, este último factor depende decisivamente del tipo de conexión a Internet. No obstante y por fortuna, parece que la banda ancha poco a poco se va abriendo camino gracias a precios que empiezan a ser razonables. Sin duda, el mejor aliciente para todos.

En este artículo vamos a explicar qué pasos deben seguir quienes deseen deleitarse con la radio y el vídeo a través de la Red. Ya no es necesario instalar costosas antenas parabólicas en el tejado. Con la ayuda de un simple PC y el software adecuado, nos recrearemos escuchando emisiones radiofónicas y contemplando programas televisivos cuyo origen está en la otra punta del planeta.

Aunque el número de aplicaciones diseñadas para permitir el acceso a este tipo de contenidos es considerable, en las siguientes líneas aprenderemos a utilizar aquellas que, por su calidad y sencillez, utilizan los cibernautas con más frecuencia.

Windows Media Player

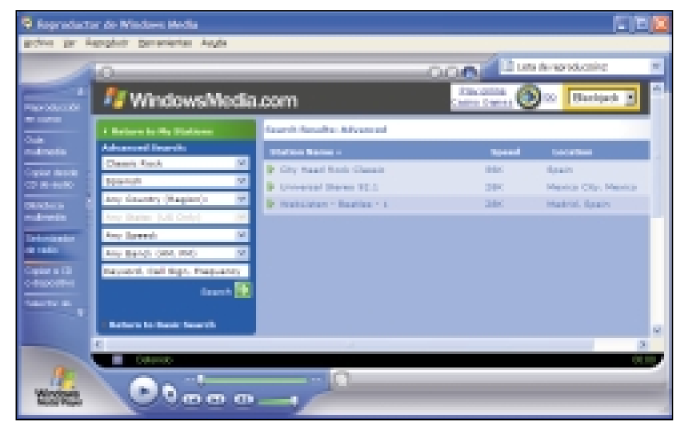
Uno de los principales desarrolladores de software del mundo no podía permanecer al margen de la que actualmente es una de las tecnologías basadas en Internet más interesantes y populares. Hablamos, por supuesto, de Microsoft. Todas y cada una de las últimas versiones de Windows han incluido esta herramienta como parte integrante del sistema operativo. Obviamente, Media Player (*www.microsoft.com/windows/windowsmedia/default.asp*) ha ido evolucionando de forma paralela a este sistema hasta llegar a ser lo que es hoy: una de las herramientas multimedia más completas y fáciles de utilizar.

Aunque su funcionalidad es realmente amplia, nos centraremos en el acceso a los contenidos que constituyen el eje central del artículo. Hemos utilizado la última versión suministrada por Microsoft, la 8, pero dada la similitud existente entre ésta y las anteriores, lo aquí explicado puede extrapolarse sin dificultad.



Lo primero que haremos es dirigirnos al módulo de sintonización de radio, que encontraremos en la barra situada en la parte izquierda de la ventana de la aplicación. Aquí, veremos un conjunto de emisoras de radio preinstaladas que podremos escuchar de forma casi inmediata. Tan sólo tendremos que hacer clic sobre la que deseemos oír para que se desplieguen una serie de opciones, entre las que encontraremos *Play*, la que nos interesa.

Pero si nuestra emisora favorita no se halla entre las anteriores, no tendremos más que recurrir a la utilidad de búsqueda integrada en Windows Media Player. Para ello, introduciremos el nombre de la emisora que deseamos localizar en el campo etiquetado con la cadena *Search Keyword* y haremos clic en el botón que, situado junto a éste, inicia el proceso de explo-

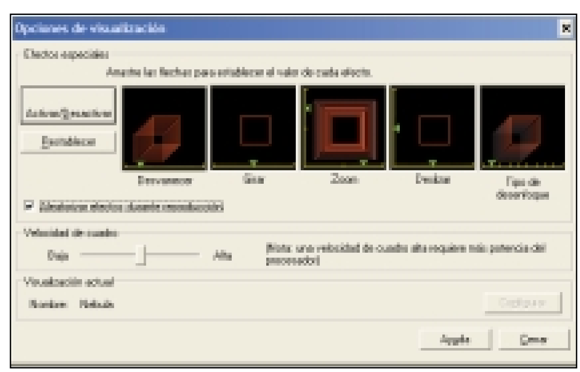


ración. En caso de que no busquemos exactamente una emisora, sino un tipo de contenidos, podemos optar por la indagación por género. Así, pincharemos en el enlace *Find More Stations* para, a continuación, seleccionar una de las opciones del menú desplegable *Browse by Genre*.

RealPlayer

Este programa es uno de las pioneros en la reproducción de contenidos multimedia en formato *streaming*. Gracias a su completa utilidad de búsqueda, RealPlayer (*www.realplayer.com*) es capaz de localizar estaciones de radio y TV en Internet de forma sencilla. Al igual que su principal rival, Windows Media Player, incorpora una serie de estaciones recomendadas por la aplicación. Pero, como hemos mencionado anteriormente, no es esta su característica más importante, sino el potente buscador que integra. Para acceder a él no tenemos más que hacer clic con el ratón en el enlace *Buscar*. Ante nosotros se desplegará una nueva ventana que alberga el habitual campo de búsqueda en el que debemos introducir la cadena de texto objeto de ésta. En la parte izquierda de esta misma ventana se ubican una serie de hiperenlaces a otras tantas páginas cuyo contenido está relacionado con el indicado en el vínculo. Si lo





que nos interesa únicamente es acceder a emisoras de radio, la eficacia de RealPlayer en este ámbito es, si cabe, mucho mayor. Haciendo clic en el icono *Sintonizador de radio* accederemos a una nueva herramienta de búsqueda más especializada en este tipo de contenidos. Para filtrar el resultado de la búsqueda, podemos especificar diversos parámetros que facilitarán en gran medida la localización de la emisora buscada. Algunos de estos son el tipo de contenidos tratados, el idioma y el país en el que se ubica. Como vemos, su utilización es tan simple como la de la aplicación de Microsoft, por lo que la verdadera dificultad no radica en saber cómo sacar provecho de la utilidad, sino en localizar aquellos contenidos que realmente nos interesan.

Televisión en la Red

La eficacia de Windows Media Player y RealPlayer a la hora de encontrar emisoras de radio que emitan en formato digital es razonablemente elevada. Sin embargo, la presencia en Internet de contenidos televisivos no es tan notoria. Por este motivo, encontrar aquellos contenidos audiovisuales que necesitamos no es sencillo. Si el resultado devuelto por estas herramientas no es el esperado, no queda más remedio que dirigirse a la página web concreta de la cadena de TV que buscamos para verificar si emiten vídeo en formato *streaming*. Paulatinamente y al igual que ha sucedido con las emisoras de radio, el número de canales de televisión que se van animando a utilizar este medio se incrementa. No ocurre lo mismo con el vídeo diferido, ya que basta con introducir el nombre de nuestro cantante preferido en un buscador para encontrar decenas de enlaces a páginas con todo tipo de contenidos, entre ellos, por supuesto, vídeos.

La clave: el streaming

Llegados a este punto cabe preguntarse: ¿cuál es el secreto de la transmisión de estos contenidos de forma eficaz? La respuesta puede sintetizarse en una sola palabra: el *streaming*. Esta tecnología permite dividir la información que se transfiere hasta nuestro ordenador en pequeños paquetes, lo que permite agilizar enormemente el proceso de transferencia. Si además tenemos en cuenta que normalmente esta información sufre un proceso de optimización que reduce su tamaño a la hora de abordar dicha transferencia, es fácil comprender el porqué de su popularidad.
Los paquetes que vamos recibiendo se almacenan con carácter temporal en un *buffer*, de forma que su contenido se va actualizando a medida que recibimos nuevos paquetes. Este es el motivo por el que es necesario realizar un *pre-buffering* o carga inicial en el *buffer* antes de comenzar el proceso de reproducción. Pero las ventajas de esta tecnología no acaban aquí. La recepción en forma de paquetes de la información ayuda al propietario de los derechos a evitar o, cuanto menos, dificultar la copia ilegal de estos contenidos. Basta con acceder a la página web de un grupo musical para escuchar con total facilidad sus temas más recientes; sin embargo, la utilización de esta tecnología impide que los almacenemos en nuestra máquina de forma ilegal. O al menos así debería ser.
Pero no todo son buenas noticias. Tal y como comentamos al principio del artículo, buena parte de la popularidad de la que goza esta tecnología en la actualidad se debe a la implantación de la banda ancha. La cuestión es: ¿es necesario tener una conexión a Internet a través de cable o líneas ADSL para disfrutar del *streaming*? Por fortuna no. Es posible disfrutar de la mayor parte de las emisiones de radio digital con una conexión a 56 Kbytes convencional. Y con una calidad realmente apreciable, libre de interferencias y demás perturbaciones. Sin embargo, la presencia de imágenes complica sustancialmente el panorama, impidiendo una reproducción fluida en la mayor parte de los casos. Excepto, claro está, si tenemos una conexión de banda ancha. A pesar de todo, es posible encontrar emisiones que, gracias a un elevado nivel de optimización, permiten afrontar el proceso de reproducción con una calidad razonable. Sin duda alguna, constituyen la excepción que confirma la regla.